Titre: Title:	Attaques informatiques sur le réseau de contrôle du trafic routier
Auteur: Author:	Marielba Urdaneta Velasquez
Date:	2018
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Urdaneta Velasquez, M. (2018). Attaques informatiques sur le réseau de contrôle du trafic routier [Mémoire de maîtrise, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/3267/

UNIVERSITÉ DE MONTRÉAL

ATTAQUES INFORMATIQUES SUR LE RÉSEAU DE CONTRÔLE DU TRAFIC ROUTIER

MARIELBA URDANETA VELASQUEZ

DÉPARTEMENT DE GÉNIE INFORMATIQUE ET GÉNIE LOGICIEL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION

DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES

(GÉNIE INFORMATIQUE)

AOÛT 2018

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

ATTAQUES INFORMATIQUES SUR LE RÉSEAU DE CONTRÔLE DU TRAFIC ROUTIER

présenté par : URDANETA VELASQUEZ Marielba

en vue de l'obtention du diplôme de : Maîtrise ès sciences appliquées

a été dûment accepté par le jury d'examen constitué de :

M. PIERRE Samuel, Ph. D., président

M. FERNANDEZ José M., Ph. D., membre et directeur de recherche

M. LEMAY Antoine, Ph. D., membre et codirecteur de recherche

M. SAUNIER Nicolas, Ph. D., membre et codirecteur de recherche

M. RICCI Patrick, ing., membre

DÉDICACE

À mon mari et mes enfants

REMERCIEMENTS

Je voudrais premièrement remercier à Dieu pour toutes les bénédictions dont il a comblé ma vie.

Je remercie mon mari et mes enfants pour tout le support, la patience et la compréhension qu'ils m'ont accordés pendant ces années d'étude. Cela a été essentiel pour ma réussite.

Je remercie mon directeur de recherche José Fernandez de m'avoir suggéré de me joindre à son équipe d'étudiants en sécurité informatique et pour le support qui m'a offert pendant mon séjour dans le laboratoire sécurité des systèmes informatiques. Je remercie aussi mon co-directeur Nicolas Saunier, pour tout son support, patience et collaboration pendant le déroulement de la recherche. Je le remercie aussi pour les nouvelles choses qu'il m'a apprises et pour le temps qu'il a consacré à lire et corriger mon travail.

Je tiens à exprimer ma sincère gratitude et mes remerciements à mon co-directeur Antoine Lemay, qui a été mon support pendant toute la recherche. J'apprécie vraiment ses visites périodiques pour suivre le projet, sa disposition à m'aider et à m'orienter, le temps qu'il a consacré à lire et à corriger les documents que je lui ai adressés, et même ses efforts et sa préoccupation pour que je trouve un travail après la fin de mon programme. Je suis tellement contente et reconnaissante de l'avoir comme co-directeur.

Je remercie les membres de jury d'avoir accepté d'évaluer ce travail.

Je remercie la Chaire Mobilité de Polytechnique Montréal et Jean-Simon Bourdeau en particulier d'avoir fait et de nous avoir fourni les affectations des données dérivées de l'Enquête Origine-Destination 2013, qui m'ont été essentielles pour modéliser le réseau de la Ville de Montréal. Je remercie la Division des Transports de la Ville de Montréal pour les informations sur les plans de feu du réseau modélisé.

Mon remerciement s'adresse aussi à mes collègues des laboratoires de recherche en réseautique et informatique mobile (LARIM) et de sécurité des systèmes informatiques (SECSI), qui m'ont accueillie chaleureusement parmi eux et qui m'ont offert leur amitié sincère et du support quand j'en ai eu besoin. Je remercie particulièrement Militza Jean qui m'a fourni tout le support moral et le soutien administratif. Sa bonne humeur, sa disposition à nous aider et les rencontres qu'elle organisait, ont rendu plus facile mon travail de recherche et cela va me manquer.

Enfin, je remercie toutes les personnes qui ont collaboré, d'une façon ou d'une autre, à l'accomplissement de ce projet.

RÉSUMÉ

Le nombre d'attaques informatiques contre les systèmes de contrôle industriels a subi une importante croissance dans les dernières années. Les systèmes de contrôle de trafic routier, étant des systèmes de contrôle industriels, sont donc exposés à des menaces informatiques qui peuvent être utilisées et exploitées par des adversaires avec le but d'altérer l'opération des feux de circulation et, en conséquence, perturber la circulation dans les réseaux routiers. Disposer d'un outil d'expérimentation qui reproduit tant un système contrôlant le trafic que le trafic dans les réseaux routiers permettrait d'évaluer le comportement de la circulation dans les réseaux routiers à l'occurrence d'attaques informatiques lancées contre le système de contrôle et ses composants. Une telle évaluation mènerait à l'identification des attaques produisant le plus d'impact, ce qui servirait à établir ou renforcer les mesures de sécurité afin de protéger le système contre ces attaques.

D'après la littérature répertoriée, un tel outil, intégrant tant le système de contrôle que le trafic routier pour les fins d'évaluer la sécurité informatique des systèmes de contrôle du trafic routier, n'a pas été implémenté. C'est pour corriger cette lacune que nous avons développé un banc d'essai qui intègre ces deux composants et qui permet de mesurer comment des attaques lancées contre le système de contrôle impactent le trafic routier. Le banc d'essai a été intégré par un logiciel qui émule les fonctions de la station centrale d'un système SCADA, des scripts développés en python qui exécutent les fonctions des PLC contrôlant les feux de circulation, et un logiciel de simulation microscopique du trafic pour la modélisation des réseaux routiers et du trafic. La fonctionnalité du banc d'essai a été validée sur trois différentes configurations des réseaux routiers, allant d'un réseau générique simple à une partie du réseau routier de la Ville de Montréal, et en exécutant divers types d'attaques et des stratégies de sélection des victimes. Les impacts des attaques ont été mesurés à partir des métriques de performance fournies par le banc d'essai, et ultérieurement, les coûts des attaques ont été estimés à partir de ces métriques.

Les expérimentations conduites tout au long de ce travail ont permis de comparer de manière quantitative l'impact des attaques exécutées ainsi que de produire une évaluation de la criticité des feux de circulation pouvant être utilisée pour prioriser les défenses contre de vraies attaques. En particulier, ces expérimentations nous ont permis de comprendre qu'une attaque informatique sur

un carrefour à feux donné peut créer des impacts sur plusieurs autres carrefours. De plus, une évaluation de différentes stratégies d'attaque a montré que les attaques ciblant les feux de circulation les plus critiques sont plus efficaces que les attaques où les cibles sont choisies de façon aléatoire, et qu'il est plus profitable pour un attaquant de changer la programmation des feux de circulation que de désactiver les feux de circulation complètement.

ABSTRACT

The number of computer-based attacks against industrial control systems has grown significantly in recent years. Road traffic control systems, being industrial control systems, are therefore exposed to cyber threats that could be used and exploited by adversaries for altering the normal operation of traffic lights and disrupting traffic in urban road networks. By having an experimental tool that reproduces the system controlling the traffic and traffic behaviour in road networks, researchers could evaluate the impact on road traffic of cyber-attacks launched against the control system and its components. Such an assessment would lead to identifying the attacks that produce the greatest impact on road traffic, and to establish or reinforce the security measures to protect the system against the most impacting threats.

According to the literature reviewed, a tool integrating both the control system and the road traffic for assessing the computer security of traffic control systems, has not been developed. For that reason, we built a cyber-physical test bed that integrates these two components and measures how attacks against the control system impact road traffic. The test bed was built integrating a software application that emulates the functions of the master station of a SCADA system, python scripts that perform the functions of the PLCs controlling the traffic lights, and a microscopic traffic simulation package for the modelling of networks and road traffic. The functionality of the test bed was validated by using three different road networks configurations, going from a simple generic network to a part of the City of Montreal's road network, and by performing several types of attacks and strategies to select the targets. The impacts of the attacks were measured against performance metrics provided by the test bed, and later, the costs of the attacks were estimated from these metrics.

The experiments conducted throughout this work provided a quantitative comparison of the impact of the attacks executed as well as an evaluation of the criticality of the traffic lights in the network. This information can be used to prioritize the defences against real attacks. In particular, these experiments showed us that an attack on a traffic light can have consequences on other crossroads. In addition, an evaluation of different attack strategies showed that attacks targeting critical signalised intersections perform better than non-targeted attacks, and that attacks modifying the timing plans of traffic lights perform better than attacks disabling the traffic light entirely.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES SIGLES ET ABRÉVIATIONS

ARP	Address Resolution Protocol
CGT	Centre de gestion du trafic
COTS	Commercial of-the-shelf
DCS	Distributed Control System
DoS	Denial of Service
FTP	File Transfer Protocol
ICS-CERT	Industrial Control Systems - Computer Emergency Response Team
IED	Intelligent Electronic Device
IFIP	International Federation for Information Processing
IP	Internet Protocol
MITM	Man in the middle
MTU	Master Terminal Unit
OPAC	Optimized Policies and Adaptive Control
OSINT	Open Source Intelligence
PLC	Programmable Logic Controller
PRODYN	Programmation Dynamique
RSH	Remote Shell
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCATS	Sidney Coordinated Adaptive Traffic System
SCOOT	Split, Cycle and Offset Optimization Technique
SM 101	Secteur Municipal 101

SUMO	Simulation of Urban Mobility
TCP	Transmission Control Protocol
TRACI	Traffic Control Interface
USB	Universal Serial Bus

CHAPITRE 1 INTRODUCTION

Les déplacements intra-urbains font partie de la vie quotidienne des individus à travers le monde. On se déplace tous les jours et le temps des déplacements varie à cause de la congestion sur le réseau routier. Pour faire une gestion efficace de la circulation et optimiser les déplacements des automobilistes, les villes se servent de systèmes de surveillance et contrôle qui permettent d'ajuster à distance la programmation des feux de circulation afin d'améliorer la circulation dans les carrefours et la mobilité des usagers. Étant donné que ces systèmes sont informatisés et accessibles à distance, ils sont les cibles d'attaques informatiques. Des individus malicieux pourraient prendre le contrôle de leurs éléments, manipuler la programmation des feux de circulation et provoquer des embouteillages sur le réseau. Un tel scénario entraînerait des effets graves sur l'économie, la sécurité des personnes et l'environnement.

Notre recherche vise à évaluer les impacts d'attaques informatiques ciblant les systèmes de contrôle du trafic routier sur la mobilité et à mesurer les coûts des attaques.

Ce premier chapitre du mémoire montre le contexte dans lequel se déroule notre recherche, la problématique étudiée et les objectifs poursuivis. L'information contenue dans ce chapitre est divisée en quatre sections. Dans la première section, nous présenterons quelques notions sur la congestion routière et la gestion du trafic. La deuxième section expose la problématique étudiée dans ce projet. Dans la troisième section nous montrerons nos objectifs de recherche, tant l'objectif général que les objectifs spécifiques. Finalement, la dernière section est dédiée à présenter la structure du mémoire.

1.1 La congestion routière et la gestion du trafic

Le trafic routier résulte des déplacements des personnes et des biens à l'intérieur des villes et des pays. De ce fait, il est lié au niveau de développement et de la prospérité des villes. Plus les villes se développent et plus leur économie augmente, plus de gens se déplacent, pour travail ou pour plaisir, et plus de biens sont livrés chaque jour. D'une certaine façon, l'augmentation de la qualité de vie, particulièrement en milieu urbain, dépend de la fluidité des transports. Toutefois, la croissance de la population et l'urbanisation continues des villes, résultantes de leur développement

économique, se traduit par une augmentation du nombre d'usagers qui doivent partager les infrastructures routières existantes. La congestion se produit lorsque le nombre d'usagers dépasse la capacité desdites infrastructures.

La congestion routière à des impacts économiques, sociaux et environnementaux. Les impacts économiques sont généralement mesurés en fonction du temps perdu, du carburant gaspillé et des émissions supplémentaires de gaz à effet de serre [1], mais d'autres études incluent aussi l'usure supplémentaire d'utilisation des véhicules [2]. La congestion augmente le temps de parcours pour la livraison des biens et des services, ce qui a une incidence directe sur leur prix final et l'économie des villes. Quant aux impacts sociaux, ceux-ci sont associés à la qualité de vie et à la santé des conducteurs et passagers des voitures retardées par la congestion ainsi que des personnes qui habitent aux alentours des zones congestionnées. Les impacts sur la santé des habitants sont liés au stress causé par les retards et aux maladies résultantes de l'exposition aux polluants dus à la combustion de carburant [3]. De tels impacts entraînent aussi des coûts économiques [4]. Par rapport à l'environnement, les polluants et les gaz à effet de serre générés par la surconsommation d'essence, ont une incidence négative sur la planète et ont été associés aux récents changements climatiques.

La congestion routière peut être de deux types : récurrente et incidente. La congestion récurrente est due au dépassement de la capacité du réseau routier à une période déterminée, comme chaque jour pendant les heures de pointe. Par contre, la congestion incidente est due aux événements imprévus, tels que les accidents dans les rues, les chantiers routiers ou des conditions météorologiques adverses (pluie, neige, brouillard, etc.). La congestion récurrente est un phénomène global, important et en croissance dans la plupart des villes du monde, et les résultats du *INRIX Global Traffic Scorecard* [5] et du *TomTom Traffic Index* [6] publiés en février 2017 le démontrent. Ces deux études ont classé Montréal, Toronto et Vancouver au sommet de la liste des villes les plus congestionnées au Canada, et parmi les cent villes les plus congestionnées du monde. Elles affirment aussi que la congestion dans ces trois villes est en croissance par rapport aux années précédentes.

Pour réduire la congestion récurrente, les villes cherchent constamment des solutions permettant d'améliorer ou de développer les infrastructures routières et les systèmes de transport en commun, ainsi que de favoriser d'autres modes de transport, tels que le covoiturage, la marche ou le vélo.

L’amélioration des infrastructures routières ne signifie pas seulement augmenter la capacité des réseaux par la construction de nouvelles routes, ou ajouter des voies aux routes existantes. Cela signifie aussi l’adoption de nouvelles technologies appliquées aux transports, comme les systèmes de transport intelligents, en particulier l’optimisation de l’opération des dispositifs de contrôle de la circulation existants, comme les feux de circulation.

Les feux de circulation sont utilisés pour contrôler le passage de plusieurs flux de circulation aux intersections lorsqu’ils sont trop complexes pour être gérés d’une autre façon (règle de priorité ou panneaux d’arrêt et de céder le passage). Les premiers feux de circulation ont été conçus en pensant à la sécurité des usagers des rues (piétons, calèches et automobilistes) lorsqu'ils franchissaient les intersections. De ce fait, les premiers mécanismes inventés possédaient un équipement limité, de telle sorte qu’ils ne pouvaient pas se connecter entre eux et ils ne pouvaient qu’attribuer un temps de passage fixe aux différents flux qui convergeaient aux intersections. Ces limitations entraînaient des inconvénients pour les usagers, par exemple lorsqu’ils devaient s’arrêter au feu rouge, même en absence de voitures traversant le carrefour.

Avec la croissance de la population des villes et des usagers des rues, la régulation du trafic routier a poursuivi un nouvel objectif : l’utilisation efficace du réseau routier. Une telle efficacité signifiait premièrement augmenter la circulation dans le réseau afin de réduire la congestion, les émissions de polluants et la perte du temps des automobilistes et passagers due aux arrêts inutiles et aux files d’attente aux feux de circulation. En conséquence, de nouveaux dispositifs, comme les détecteurs de présence des véhicules, et de nouvelles stratégies de régulation, comme l’opération conjointe d’un ensemble de carrefours à feux, ont été adoptés. L’intégration des détecteurs permet une régulation adaptative du trafic, en permettant aux feux de circulation d’ajuster le temps de passage des flux en fonction des conditions réelles du trafic aux carrefours. Pour sa part, l’opération simultanée d’un ensemble de carrefours à feux permet de maximiser le nombre de véhicules traversant un corridor ou un réseau routier, tout en minimisant le nombre d'arrêts et le retard et en réduisant la consommation d'essence et les émissions de polluants.

Les premiers systèmes de régulation de la circulation basée sur des ordinateurs sont apparus pendant les années 1960. Ils étaient typiquement composés de contrôleurs de feux de circulation et de détecteurs placés sur le terrain, d’un réseau de communication et d’une station centrale [7]. Ils opéraient dans des environnements isolés et utilisaient des logiciels, matériels et protocoles de

communication propriétaires. L'échange d'information entre l'équipement sur le terrain et la station centrale se faisait à travers des réseaux de communications dédiés utilisant des moyens physiques pour transmettre l'information. Avec le développement des microprocesseurs et des technologies de l'information et de la communication, ces systèmes ont évolué vers les systèmes de contrôle de trafic modernes. Les systèmes actuels sont plus interconnectés qu'avant et sont devenus accessibles à distance. Ils utilisent des réseaux de communication sans fil, l'Internet, les protocoles de communication basés sur des standards communs et les systèmes d'exploitation et des technologies commerciales afin d'assurer l'intégration et l'interopérabilité de leurs différents composants [8].

La gestion du trafic actuelle s'appuie sur l'utilisation de capteurs qui saisissent les conditions réelles du trafic, des feux de circulation qui ajustent leur programmation en fonction desdites conditions, et des logiciels spécialisés, qui font le traitement de nombreuses informations reçues du terrain et calculent de façon continue la programmation optimale des feux de circulation. Ces éléments sont reliés entre eux à travers d'un réseau de communications qui permet l'échange bidirectionnel d'information entre la station centrale et l'équipement sur le terrain. En conséquence, un opérateur à la station centrale peut connaitre en temps réel les conditions du trafic sur le réseau et aussi l'état et la programmation des feux de circulation. Les nouvelles programmations, une fois calculées, peuvent être téléchargées aux feux de circulation depuis la station centrale, soit en temps réel, périodiquement ou par commande de l'opérateur.

L'optimisation de l'opération des feux de signalisation peut avoir un impact direct et immédiat sur la circulation et l'utilisation efficace du réseau routier. Des mesures, telles qu'ajuster périodiquement la programmation des feux de circulation en fonction des débits de trafic existants et mettre à niveau l'équipement sur le terrain, amènent à une réduction importante des retards, de la consommation d'essence et des émissions de polluants. Par exemple, entre 2007 et 2009 le Département des transports de Boston a réglé la programmation de soixante feux de circulation dans la zone de Back Bay, dans le cadre d'un projet d'amélioration de la circulation et de la sécurité dans son réseau routier. Comme résultat, ils ont atteint une réduction par année de 89 400 heures de retard, de 5,46 tonnes métriques des émissions de polluants et de 54 860 gallons de consommation d'essence. Toutes ces réductions ont entraîné une économie d'à peu près 2 millions USD par année [9]. Un autre exemple est le projet d'optimisation de la programmation et de la coordination de feux de circulation à la ville de Bloomington, dans l'état du Minnesota. Ce projet

visait à ajuster la programmation de 61 feux de circulation de la ville et à implémenter la coordination des feux aux corridors, si c'était convenable. Mais, le rapport émis en 2012 ne montre que les résultats des modifications faites à 22 feux de circulation, se trouvant dans trois zones d'étude : Normandale Boulevard (avec neuf feux de circulation), East Bush Lake Road (avec dix feux de circulation) et Mall of America (avec trois feux de circulation). Comme résultat, le nombre d'arrêts dans les trois zones s'est réduit en moyenne de 10,7 %, le retard s'est réduit de 12,1 % à la première zone et est resté constant dans les deux autres zones, et la consommation d'essence dans les trois zones s'est réduite en moyenne de 3 %. Ces réductions ont mené à une économie de 2,7 millions USD par année [10]. Ces études démontrent l'important coût économique lié à un manque d'optimisation des systèmes de régulation de la circulation.

Mais de tels résultats ne sont pas garantis. En 2006 deux ingénieurs du centre de gestion du trafic de Los Angeles, dans l'état de la Californie, ont modifié la programmation de quatre feux de circulation se trouvant sur quatre des intersections les plus achalandées de la ville [11] [12]. Cette action a eu lieu dans le cadre d'une proteste des travailleurs du trafic et a produit des embouteillages qui ont duré quelques jours. Lesdits ingénieurs ont altéré la programmation des feux de circulation de sorte que le temps du feu rouge pour les voies avec le débit le plus élevé était considérablement plus long que celui attribué aux voies avec la circulation la plus faible. Bien que ce soit un exemple d'une attaque perpétrée par des attaquants internes, où les responsables ont été identifiés et condamnés, le plus remarquable dans l'exemple est le fait qu'altérer la programmation des feux de circulation peut aussi entraîner des conséquences néfastes sur la circulation routière.

1.2 Problématique

Avec l'incorporation des technologies de l'information et de la communication à la gestion du trafic routier et l'utilisation de plus en plus fréquente des réseaux de communication sans fil pour interconnecter les différents éléments des systèmes, les systèmes de contrôle du trafic routier actuels sont accessibles à distance et susceptibles de subir des attaques informatiques.

En 2014, Ghena *et al.* [13] et Cerrudo [14], ont évalué la sécurité des éléments des systèmes de contrôle de trafic routier couramment déployés aux États-Unis. Ils ont détecté des vulnérabilités qui leur ont permis d'accéder à des éléments du système et d'altérer l'opération des feux de circulation à volonté.

Spécifiquement, Ghena et son équipe ont remarqué que :

- Le système étudié utilisait un réseau de communication sans fil pour connecter les contrôleurs de feux de circulation avec la station centrale et l'information échangée entre eux n'était pas chiffrée.
- Le routeur du réseau de communication et les contrôleurs des feux de circulation utilisaient les noms d'usager et les mots de passe par défaut fournis par leurs fabricants.
- Il était possible d'accéder aux contrôleurs des feux de circulation à l'aide d'un port de débogage qui restait toujours ouvert.

En travaillant en collaboration avec les autorités de la ville, Ghena et son équipe ont exploité ces vulnérabilités pour accéder au réseau de communication et aux contrôleurs de feux de circulation. Une fois l'accès obtenu, ils ont manipulé les feux de circulation. Ils ont aussi expliqué que ces conditions permettraient à un adversaire d'exécuter des attaques de déni de service et des attaques ciblant l'infrastructure routière. D'un côté, l'attaquant pourrait manipuler les feux de circulation pour mettre l'ensemble de feux en rouge. Une telle condition empêcherait le contrôle du trafic au carrefour et produirait de la confusion chez les conducteurs. Cela serait une attaque de déni de service. Quant à l'infrastructure routière, l'attaquant pourrait altérer la programmation d'un feu de circulation opérant en coordination avec des carrefours à feux voisins, ce qui augmenterait la congestion dans le réseau.

Pour sa part, Cerrudo a constaté que le système sans fil de détection de présence des véhicules, installé dans 40 villes aux États-Unis et dans des villes de 9 autres pays, manquaient de mécanismes tant d'authentification que de chiffrement de la communication. Dans cette condition, il était facile d'accéder aux composants du système pour modifier leur configuration, et d'intercepter et de manipuler l'information envoyée aux contrôleurs des feux de circulation.

En conséquence, un adversaire profitant de ces vulnérabilités pourrait attaquer des feux de circulation d'une ville et impacter la circulation. Toutefois, il est difficile de déterminer précisément quelles seraient les conséquences de telles attaques. Nous proposons d'évaluer les impacts d'attaques cybernétiques visant les systèmes de contrôle du trafic routier sur la congestion routière et de mesurer leurs coûts. Cette meilleure compréhension des impacts permettra une évaluation quantitative du risque associé à ce type de menace.

1.3 Objectifs

L'objectif principal de ce mémoire est de mesurer l'impact des attaques informatiques contre le réseau de contrôle du trafic routier. Atteindre cet objectif requiert de disposer d'un outil qui nous permet de reproduire des attaques informatiques contre le système et les éléments de contrôle du trafic routier et de mesurer l'impact des attaques. C'est dans cette optique que nous avons défini les objectifs spécifiques de recherche suivants :

1. Développer un banc d'essai pour reproduire les systèmes contrôlant le trafic dans des réseaux routiers.
2. Reproduire expérimentalement des attaques informatiques sur les contrôleurs de feux de circulation d'un réseau routier.
3. Reproduire expérimentalement l'état de la circulation dans un réseau routier de Montréal en conditions normales et pendant une attaque informatique sur les feux de circulation.
4. Mesurer les coûts économiques des attaques, en fonction de l'augmentation du retard résultant de l'attaque sur le réseau.

L'avantage premier d'un tel outil est de mesurer les coûts qui résulteraient du temps supplémentaire subit par les conducteurs dans un réseau routier pendant une attaque. Cependant, il offrira aussi un scénario expérimental permettant de reproduire différents types d'attaques, dans différentes conditions du trafic, ce qui servirait à déterminer les vecteurs d'attaque et les cibles qui produiraient le plus d'impact négatifs sur la circulation. Avec cette information, les autorités pourraient envisager des stratégies de défense efficaces pour renfoncer la sécurité informatique des réseaux et de leurs composants les plus vulnérables. Aussi, elles pourraient identifier et établir les mesures adéquates pour minimiser l'impact physique des attaques, c'est-à-dire l'impact sur la circulation routière. En outre, elles pourraient déterminer à l'avance la meilleure stratégie de mitigation à implémenter, selon l'impact des attaques, ce qui leur faciliterait la prise de décisions dans le cas où de vraies attaques se produiraient.

1.4 Organisation du mémoire

Ce mémoire est composé de 8 chapitres, organisés comme suit :

Le Chapitre 1, l'introduction, a servi à présenter le contexte de la circulation routière et sa relation avec notre recherche, ainsi qu'à introduire la problématique abordée et montrer tant l'objectif général que les objectifs spécifiques de la recherche.

Le Chapitre 2 présente le cadre théorique du contrôle de trafic routier, en montrant les différents éléments, paramètres de contrôle, architectures et stratégies de contrôle des systèmes actuels de contrôle du trafic.

Le Chapitre 3 est consacré à la sécurité des systèmes de contrôle industriels. Nous y présentons les notions basiques des systèmes de contrôle industriels, incluant leurs architectures et composants. Nous expliquons aussi pourquoi les systèmes actuels sont plus susceptibles qu'auparavant à subir des attaques informatiques et décrivons les différentes attaques et menaces auxquelles ils sont exposés. Cette information est complémentée avec des exemples de vraies attaques informatiques qui ont été lancées contre différents systèmes contrôlant des infrastructures critiques dans différentes parties du monde. Finalement, nous présentons une sélection des travaux antérieurs qui ont portée sur la sécurité informatique des systèmes de contrôle industriels et des systèmes de contrôle du trafic routier.

Le Chapitre 4 montre la démarche du travail fait pour développer le banc d'essai et sa relation avec les objectifs de recherche énoncés.

Le Chapitre 5 présente l'article « A cyber-physical test bed to measure the impacts of cyber attacks in urban road networks », qui a été présenté à la « Twelfth IFIP WG 11.10 International Conference on Critical Infrastructure Protection », en mars 2018. Cet article décrit le banc d'essai que nous avons développé, incluant ses composants, les critères de performance considérés pour sélectionner les éléments qui le composent, et les différentes configurations utilisées et tests exécutés, tant pour valider sa correcte opération que pour reproduire des attaques informatiques sur des réseaux routiers et mesurer leurs impacts.

Le Chapitre 6 présente des aspects méthodologiques et des résultats complémentaires qui n'ont pas été inclus dans l'article. Cela corresponde à la démarche additionnelle que nous avons empruntée afin reproduire expérimentalement l'état de la circulation dans un réseau routier de Montréal, en

conditions normales et pendant une attaque informatique contre les feux de circulation, et de mesurer les coûts des attaques.

Le Chapitre 7 présente une discussion générale portant sur l'analyse critique de la méthodologie adoptée et sa pertinence avec les objectifs de la recherche.

Finalement, les Chapitre 8 présente une synthèse de toute la démarche exécutée, les limitations du banc d'essai développée, les contributions du travail de recherche et des améliorations et des pistes pour des travaux futurs.

CHAPITRE 2 NOTIONS DE LA RÉGULATION DU TRAFIC ROUTIER

Dans ce chapitre nous présentons des notions élémentaires de la régulation de la circulation aux carrefours afin de faciliter la compréhension du contenu de ce mémoire. Dans un premier temps nous montrerons les éléments constituant un carrefour à feux et leurs caractéristiques générales. Ensuite, nous définirons les paramètres utilisés pour contrôler le trafic routier. Par la suite, nous expliquerons les différentes stratégies de régulation du trafic. Puis, nous décrirons les différents systèmes de contrôle de trafic, et finalement nous montrerons les architectures de ces systèmes.

2.1 Les feux de circulation

Les feux de circulation, ou feux de signalisation, sont des dispositifs électriques qui contrôlent le trafic aux carrefours. Ils permettent aux usagers des rues (piétons, automobilistes et cyclistes) de partager en sécurité une partie du réseau routier, généralement aux intersections, en leur attribuant différentes périodes de temps pour qu'ils puissent les traverser. Avec une programmation adaptée aux conditions du trafic aux carrefours, les feux de signalisation contribuent à améliorer la circulation dans le réseau et la sécurité des usagers des rues.

La Figure 2.1 montre les composants d'un feu de circulation. Les têtes de feux hébergent des ampoules colorées (verte, jaune et rouge) qui indiquent aux automobilistes le moment de traverser le carrefour ou de s'arrêter, tandis que les feux piétons régulent le passage des piétons. Le contrôleur de feux est le cerveau du carrefour à feux. Il est le responsable de commuter les feux qui attribuent le droit de passage, la priorité, aux différents flux dans le carrefour. Sur certains carrefours, des détecteurs captent la présence de véhicules, piétons ou cyclistes aux approches du carrefour. Ils communiquent avec le contrôleur de feux pour lui fournir l'information saisie. Le contrôleur de feux peut alors utiliser l'information fournie pour réguler le trafic au carrefour.

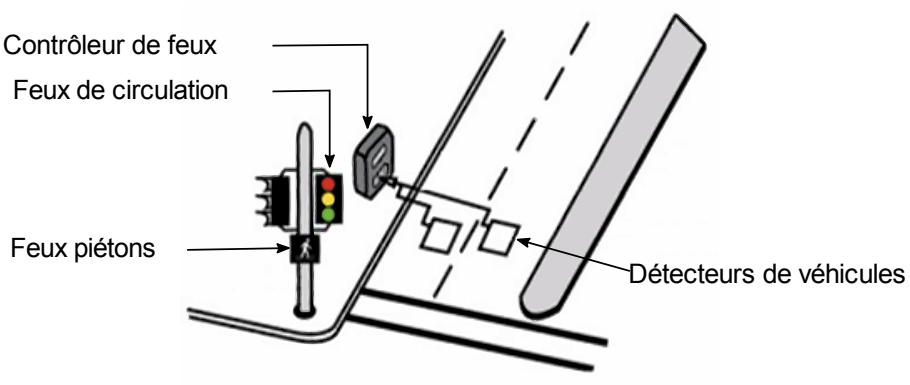


Figure 2.1 : Composants d'un feu de circulation (adaptée de [15])

2.1.1 Contrôleurs de feux de circulation

La plupart des contrôleurs de feux de circulation modernes contiennent les éléments suivants [16]:

- Interface usager (écran et clavier) pour la maintenance et la configuration ;
- Une unité de traitement centrale muni d'un microprocesseur, mémoire, etc. ;
- Ports série, Ethernet et USB pour communiquer avec des dispositifs externes, tels qu'une unité de contrôle centrale ou un ordinateur local (laptop) pour les tâches d'entretien ;
- Une unité d'alimentation en énergie ;
- Des processeurs de communication série (optionnels), tels que des modems FSK ou RS232.

Les contrôleurs sont placés à l'intérieur d'un cabinet qui est rattaché au carrefour. En plus des contrôleurs, ce cabinet héberge aussi :

- Des interrupteurs pour commuter les feux ;
- Une unité de détection, qui reçoit l'information saisie par les capteurs, le cas échéant ;
- Une unité de gestion des conflits (« Malfunction Management Unit ») ;
- Dispositifs optionnels pour la communication avec des dispositifs externes, tels que modem FSK, émetteur-récepteur à fibre optique ou sans fil, commutateur Ethernet, etc.

L'unité de gestion des conflits est responsable de détecter et de répondre aux conditions anormales liées à l'opération du contrôleur et des commutateurs des feux, au câblage et au voltage d'opération des éléments du cabinet. Elle est programmée avec les combinaisons permises des feux et le temps

minimal et maximal de durée de chaque phase. En cas d'une panne du contrôleur ou d'une combinaison de feux non autorisée, comme le feu vert pour toutes les approches, l'unité de gestion des conflits met le feu de circulation en mode défaut. Étant en mode défaut, l'unité de gestion des conflits met tous les feux en rouge clignotant. Une fois le mode défaut activé, il faut l'intervention manuelle d'un opérateur au carrefour pour remettre le feu de circulation en opération normale.

2.1.2 Détecteurs

Les détecteurs sont des dispositifs qui indiquent l'existence de certains phénomènes physiques. Ils sont généralement utilisés pour détecter la présence d'un objet ou d'une substance particulière à partir du phénomène physique capté et d'émettre un signal en réponse. Les détecteurs utilisés pour saisir et surveiller les conditions du trafic requièrent d'un transducteur, qui détecte le passage au la présence des véhicules, d'un dispositif de traitement des signaux, qui converti ce qui est généré par le transducteur en un signal électrique, et d'un dispositif de traitement de l'information [17]. Ce dernier se compose généralement de matériel et logiciel qui convertissent les signaux électriques en des paramètres du trafic ; il peut être intégré aux capteurs ou être un dispositif externe. La présence des véhicules, la vitesse, le nombre de véhicules et le taux d'occupation, entre autres, sont des exemples de paramètres du trafic.

Ils existent deux technologies différentes des détecteurs utilisés pour saisir et surveiller les conditions du trafic : les détecteurs enfouis dans la chaussée et les détecteurs aériens [7] [17]. Les détecteurs installés dans la chaussée sont plus précis que les détecteurs aériens, mais leur installation et leur réparation nécessitent de fermer les voies où ils sont installés à la circulation. Les boucles d'induction et les détecteurs magnétiques appartiennent à cette catégorie. Pour leur part, les détecteurs aériens sont plus faciles à installer et à maintenir que les détecteurs installés dans la chaussée. Par contre, ils sont plus coûteux que les détecteurs installés dans la chaussée et la précision de la détection est influencée par les conditions environnementales. Les radars, les détecteurs infrarouges, les détecteurs ultrasoniques et les caméras vidéo sont des exemples de détecteurs aériens. Cependant, avec l'évolution des technologies de la communication, les réseaux de capteurs aériens sans fil sont à nos jours de plus en plus utilisés pour la détection des conditions du trafic [18] [19] [20] [21].

Selon leur fonction, les détecteurs se divisent en trois catégories : détecteurs de présence, détecteurs par pulsation et détecteurs du système [22]. Les détecteurs de présence captent les véhicules

(arrêtés ou en mouvement) qui entrent dans leur zone de détection. Ces capteurs sont généralement utilisés pour commuter les feux en fonction des véhicules qui attendent aux approches des carrefours. Les détecteurs par pulsation génèrent une pulsation de courte durée lors qu'ils détectent un véhicule. Ils sont habituellement utilisés pour faire le comptage des véhicules sur les approches des carrefours. Finalement, les détecteurs du système saisissent l'information concernant la vitesse, le débit, le taux d'occupation des voies et la longueur des files d'attente. Ce type d'information est utilisée par des algorithmes de contrôle du trafic pour faire une régulation qui s'ajuste le mieux au trafic réel.

Ils existent aussi des détecteurs qui déterminent la présence des véhicules d'urgence (pompiers ou ambulances) à proximité des carrefours à feux. Ils alertent les contrôleurs de feux sur la présence des véhicules de secours. Alors, les contrôleurs de feux adaptent leur programmation afin de favoriser la circulation de ces véhicules. Des détecteurs acoustiques et optiques sont utilisés pour accomplir cette fonction.

2.2 Paramètres de contrôle

Un flux ou courant représente différents mouvements (ensemble de véhicules avec même origine et destination) réunis sur une même voie. Les flux peuvent correspondre à des mouvements directs (tout droit), des mouvements de tourne-à-gauche ou de tourne-à-droite. Ils existent aussi les flux de piétons, des cyclistes et de voitures. Lorsque les trajectoires de deux ou plusieurs flux se croisent à l'intérieur du carrefour, les flux sont considérés conflictuels ou antagonistes. Dans ces cas, il faut leur accorder une priorité (droit de passage) pour qu'ils puissent traverser le carrefour en sécurité. Selon les caractéristiques des intersections, le droit de passage peut être géré par des règles de priorité, des panneaux d'arrêt et de cédez le passage ou des feux de circulation.

Aux intersections munies de feux de circulation, le contrôleur de feux attribue le droit de passage en allouant un temps de feu vert successivement à chacun des flux. L'information concernant le nombre de flux, leur ordre de passage (séquence) dans le carrefour et la durée du feu vert pour chaque flux fait partie du ***plan de feu***. Celui-ci définit comment le contrôleur régule le trafic. Les plans des feux contiennent les paramètres de contrôle suivants : les phases, les intervalles, la durée des phases, le cycle de feu, la durée du cycle et le décalage.

Selon le « Traffic control systems handbook » [23], ***une phase*** est le droit de passage dans le carrefour d'un flux ou de plusieurs flux simultanés. Chaque phase est composée d'un intervalle de feu vert, d'un intervalle changement de phase (feu jaune) et d'un intervalle de dégagement (feu rouge dans l'ensemble de feux). ***Un intervalle*** est la période du cycle de feux pendant laquelle les feux ne changent pas. ***La durée de phase*** (en anglais « split ») s'agit du temps, ou du pourcentage de la durée du cycle, attribué à chacune des phases. ***Le cycle de feu*** correspond à l'enchaînement de toutes les phases permettant la circulation de tous les flux dans le carrefour. Pour sa part, ***la durée du cycle*** est le temps requis pour compléter le cycle de feu. Finalement, ***le décalage*** (an anglais « offset ») est le temps qui s'écoule entre le début des cycles de deux carrefours à feux consécutifs se trouvant sur un corridor ou réseau routier. Ce paramètre est utilisé pour favoriser le déplacement d'un peloton de véhicules dans le corridor, en minimisant le nombre d'arrêts aux carrefours à l'intérieur du corridor.

La Figure 2.2 montre, à gauche, un exemple des flux convergeant à un carrefour à 4 branches. On y distingue 4 flux directs et 4 flux de tourne-à-droite. La même figure montre, à droite, le regroupement de ces flux en phases. Ensuite, la Figure 2.3 montre les éléments contenus dans le plan de feu utilisé pour contrôler le trafic audit carrefour.

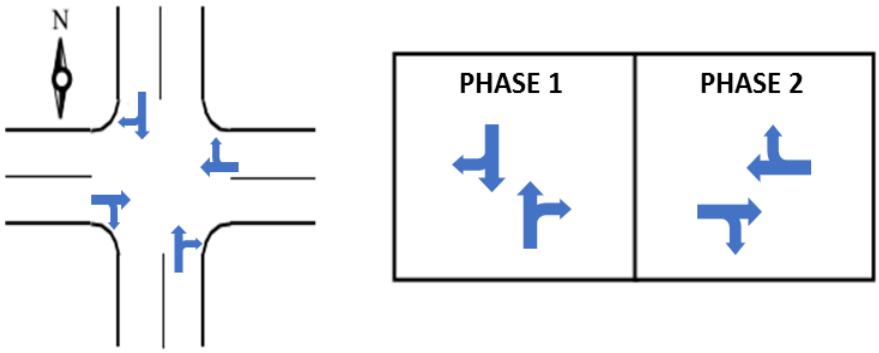


Figure 2.2 : Flux à une intersection à 4 branches et regroupement des flux en phases (adapté de [16])

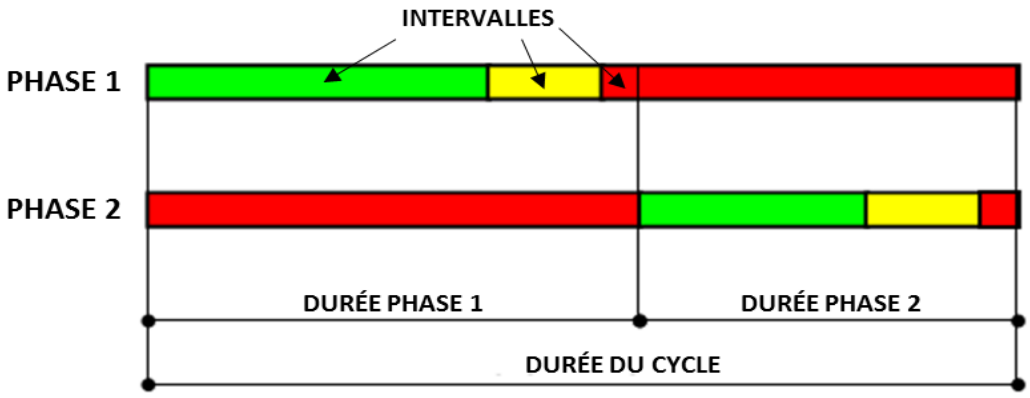


Figure 2.3 : Éléments d'un plan de feu (adapté de [16])

Les plans de feux sont calculés par les ingénieurs du trafic en tenant compte de la demande et des conditions du trafic à chaque carrefour. Le calcul consiste à déterminer la durée du cycle, la durée des phases et les décalages optimaux pour maximiser la capacité du réseau routier et minimiser les retards dans les trajets causés par les feux de circulation.

Une fois calculés, les plans sont stockés dans les contrôleurs de feux pour leur utilisation. Le cas le plus simple est celui d'un contrôleur avec un seul plan de feu. S'il y en a plusieurs, le contrôleur sélectionne le plan de feu à utiliser, à un moment déterminé, soit de façon interne ou externe. La sélection interne est basée sur une planification horaire établie à l'avance par l'opérateur et qui est téléchargée dans le contrôleur. Cette planification est générée à partir des données historiques des conditions du trafic. Elle contient le plan à utiliser pendant les différentes périodes de la journée ou les jours de la semaine. Au moins trois périodes de la journée sont prises en compte dans la planification : les heures de pointe du matin, de l'après-midi et les heures hors des heures de pointe. Des dates spéciales, telles que des fêtes connues ou le début et la fin des périodes de vacances peuvent aussi être considérées dans la planification. Quant à la sélection externe, elle est faite par commande de l'opérateur ou d'un contrôleur maître, qui dit au contrôleur d'utiliser un plan déterminé. Cette stratégie requiert un lien de communication entre le contrôleur et les dispositifs de commandement externes. Dans ce cas, la sélection répond aux conditions réelles du trafic, captées par les détecteurs, ou aux situations imprévues, telles que des accidents, détours, la circulation des véhicules d'urgence, etc. En cas de pannes de communication, le contrôleur reprend automatiquement la méthode de sélection interne [24].

2.3 La régulation du trafic routier

Les carrefours à feux peuvent opérer de façon isolée ou en coordination avec d'autres carrefours à feux. Dans le premier cas, les contrôleurs de feux de circulation ne tiennent pas compte des carrefours à feux voisins, mais des conditions au carrefour où ils sont installés. Dans le deuxième cas, un ensemble de carrefours à feux se trouvant sur un même corridor routier ou sur un réseau de blocs voisins est contrôlé de façon coordonnée. Cette stratégie vise à favoriser la circulation continue d'un flux important de véhicules sur le corridor ou le réseau.

Le trafic aux carrefours isolés est régulé en utilisant soit des plans de feux prédéterminés ou la commutation dynamique des feux. Un plan de feu prédéterminé ne tient pas compte des conditions réelles du trafic au carrefour. Ce type de régulation est utilisé aux intersections où les conditions du trafic sont prévisibles.

Pour sa part, la commutation dynamique ou régulation adaptative des feux s'appuie sur des détecteurs placés sur les approches du carrefour. Dans ce cas, le contrôleur modifie les feux en fonction de l'information du trafic reçue en temps réel des détecteurs. En conséquence, le nombre de phases, leur ordonnancement et leur durée peuvent varier selon les conditions du trafic. Cette stratégie de contrôle est aussi divisée en deux catégories : régulation semi-adaptative et complètement adaptative. La commutation semi-adaptative est généralement utilisée aux carrefours où les débits sur les différentes approches sont très différents. Les détecteurs sont placés sur les approches ayant le débit le plus faible (approches secondaires). Les véhicules aux approches avec le débit le plus élevé ont le droit de passage en permanence, à moins que la présence des véhicules ou piétons sur les approches secondaires ne soit détectée. Lorsque le droit de passage est donné aux véhicules sur les approches secondaires, la durée de cette phase varie d'un temps de vert minimal à un temps de vert maximal. La commutation complètement adaptative, par contre, requiert des détecteurs sur toutes les approches du carrefour. Cela signifie que le droit de passage de tous les flux est attribué en fonction des véhicules détectés. Généralement, la durée de chaque phase varie entre une durée de vert minimale et maximale, avec des extensions selon la détection continue de véhicule sur l'approche. Cette stratégie est généralement utilisée aux carrefours isolés où le débit et les conditions du trafic varient de manière significative pendant la journée [25].

Dans les cas de la coordination des carrefours à feux sur des corridors ou de petits réseaux routiers, les paramètres de contrôle des feux sont calculés en visant à favoriser la création des ondes vertes.

Cela signifie qu'une flotte de véhicules se déplaçant à une vitesse déterminée a le droit de passage dans plusieurs feux de circulation successifs à l'intérieur du corridor ou réseau. Pour atteindre cet objectif, il faut faire le calcul et la sélection adéquats des paramètres de contrôle des plans de feux des carrefours. Ces paramètres sont calculés de telle sorte qu'ils permettent d'atteindre les objectifs de la régulation du trafic tant à chaque carrefour que dans l'ensemble (corridor ou réseau) [16]. Alors, ils sont calculés en respectant les consignes suivantes :

- La durée du cycle doit être commune pour tous les feux de circulation dans le réseau coordonné. Si les conditions du trafic à chaque carrefour obligent à utiliser différentes durées du cycle, la durée du cycle des carrefours du réseau doit être proportionnelle à la durée du cycle de tous les carrefours à feux. Alors, la durée du cycle du système sera la durée du cycle la plus longue.
- La durée des phases (« split ») est calculée pour toutes les phases de tous les carrefours à feux individuellement.
- Dans le plan de feu de chaque carrefour, il faut choisir une phase coordonnée afin d'établir une référence pour le système. Généralement, la phase coordonnée choisie est celle qui correspond au flux le plus important. Cette phase doit être fixe dans le plan de feu de tous les carrefours.
- Le décalage (« offset ») est calculé pour chacun des carrefours. Sa valeur correspond à la durée entre le début de la phase coordonnée à un carrefour déterminé et le début de la phase coordonnée à un autre carrefour du réseau considéré comme le carrefour de référence.

2.4 Systèmes de contrôle du trafic routier

Pour implémenter la coordination entre carrefours il existe différentes techniques. Cette section présente les différents types des systèmes de contrôle du trafic routier et les techniques utilisées pour implémenter la coordination (tirée de [16] [24]).

2.4.1 Systèmes de coordination basés sur l'heure (« Time-Based coordinated systems »)

Dans ce type de système les contrôleurs de feux de circulation des carrefours ne sont pas reliés entre eux. La coordination est accomplie en réglant les horloges de chaque contrôleur de feux à la

même heure. Pour corriger la dérive temporelle des horloges et maintenir la coordination, les horloges de tous les contrôleurs sont remises périodiquement à une heure commune. Des récepteurs GPS sont communément utilisés pour synchroniser l'heure des contrôleurs.

Ce type de système utilise les plans de feux prédéterminés pour réguler le trafic. Les plans de feux sont calculés à une station centrale mais déposés directement dans les contrôleurs aux carrefours. La sélection des plans de feux se fait par la méthode interne en respectant une planification horaire aussi déposée dans les contrôleurs. Cette technique s'appelle choix des plans de feu selon l'horaire. Pour garantir la coordination, tous les carrefours à feux suivent la même planification horaire pour la sélection des plans de feux.

La station centrale ne possède pas d'information en temps réel ni sur l'état du trafic ni sur l'état de l'équipement sur le terrain.

2.4.2 Systèmes interconnectés

Contrairement aux systèmes antérieurs, dans les systèmes interconnectés, les carrefours à feux sont connectés entre eux soit par câbles ou par communication sans fil. Ils communiquent aussi avec une station centrale.

Similairement aux systèmes basés sur l'heure, la régulation du trafic s'appuie sur les plans de feux prédéterminés calculés à la station centrale. Par contre, les systèmes interconnectés permettent de télécharger les plans de feux à distance dans les contrôleurs de feux. En plus, un opérateur à la station centrale peut consulter les plans de feux stockés dans les contrôleurs. La sélection des plans de feux peut se faire en respectant une planification horaire préétablie (sélection interne) ou par l'action de l'opérateur (sélection externe).

La station centrale surveille l'état de l'équipement sur le terrain et l'opération des feux de circulation. Si le système est muni de détecteurs, l'information récoltée est utilisée par l'opérateur pour surveiller le trafic et faire la planification.

2.4.3 Systèmes réagissant au trafic (« Traffic responsive systems »)

Ces systèmes ont les caractéristiques des systèmes interconnectés mais ils s'appuient sur la détection des conditions du trafic pour sélectionner les plans de feux. Comme dans les systèmes interconnectés, les plans de feux sont calculés à la station centrale et téléchargés dans les

contrôleurs de feux. Par contre, la sélection des plans se fait soit à la station centrale ou à un contrôleur maître sur le terrain, dépendant de l'architecture du système. Le contrôleur maître communique avec tous les contrôleurs de feux du système pour garantir la coordination. Lorsqu'un nouveau plan est sélectionné, la station centrale ou le contrôleur maître (selon le cas) envoie une commande à tous les contrôleurs de feux pour qu'ils changent le plan simultanément, généralement au cycle suivant.

Les détecteurs mesurent les débits et les taux d'occupation dans toutes les directions et toutes les voies. Cette information est ensuite utilisée par des algorithmes de contrôle qui sélectionnent le plan de feu. Selon l'architecture utilisée, les algorithmes de contrôle s'exécutent à la station centrale ou au contrôleur maître. De plus, la station centrale stocke l'information du trafic, l'affiche et l'analyse pour déterminer s'il est nécessaire de modifier les paramètres des plans de feux et le type de modifications à faire.

Aux emplacements où les conditions du trafic varient significativement et de façon non prévisible, ces systèmes performent mieux la régulation du trafic que les systèmes utilisant une planification horaire pour la sélection des plans de feux.

2.4.4 Systèmes adaptatifs au trafic (« Traffic adaptive systems »)

Les systèmes décrits précédemment utilisent un ou deux plans de feu précalculés pour adapter la régulation aux conditions du trafic, tandis que les systèmes adaptatifs au trafic se caractérisent par leur ajustement automatique et en temps réel de la durée du cycle, les durées des phases et le décalage selon les conditions réelles du trafic. Cette technique amène à une augmentation de la vitesse de déplacement, ce qui se traduit par une réduction des retards.

Ce type de système utilise des algorithmes plus sophistiqués et demande plus d'information du trafic que les systèmes décrits précédemment. Une coordination performante dépend de la précision et de la disponibilité des données récoltées par les détecteurs.

Parmi les systèmes de contrôle adaptatifs les plus utilisés on peut mentionner :

- SCOOT (« Split, Cycle and Offset Optimization Technique ») [26] développé par le « Transport and Road Research Laboratory, TRRL », en Grande-Bretagne, entre 1972 et 1980;

- SCATS (« Sydney Coordinated Adaptive Traffic System ») [27] installé à Sydney, Australie, au début des années 1980;
- OPAC (« Optimized Policies for Adaptive Control ») [28] développé aux États-Unis par l'Université de Lowell, Massachusetts, dans le cadre d'un projet mené par le département américain des Transports (« U.S. Department of Transportation »);
- PRODYN (Programmation Dynamique) [29] développé en France par le Centre d'Études et de Recherche de Toulouse (CERT).

2.5 Architecture des systèmes de contrôle de trafic routier

En général, les systèmes de contrôle de trafic routier sont constitués par des contrôleurs de feux aux intersections, d'une station centrale pour la gestion du trafic et d'un réseau de communication qui relie les feux de circulation et la station centrale. Cependant, les architectures prédominantes dans les systèmes en usage sont des architectures réparties en deux et trois niveaux.

2.5.1 Systèmes répartis en trois niveaux (« closed loop systems »)

Ces systèmes possèdent une architecture où la logique de contrôle est distribuée sur trois niveaux: des contrôleurs de feux (contrôleurs locaux), un contrôleur maître et une station centrale ou Centre de Gestion du Trafic (CGT) [24] [25]. La Figure 2.4 montre les éléments typiques de ces systèmes.

Les contrôleurs des feux reçoivent l'information des conditions du trafic en provenance des détecteurs et l'envoient au contrôleur maître. Celui-ci se sert de cette information pour déterminer le plan de feu qui répond au mieux aux conditions du trafic et envoie des commandes aux contrôleurs des feux du système pour leur indiquer de changer de plan. Le contrôleur maître envoie aussi des pulses de synchronisation aux contrôleurs des feux pour garantir l'heure et la coordination du système. De sa part, la station centrale calcule les paramètres des plans de feux et la planification horaire à partir des conditions du trafic, envoyées par le contrôleur maître, et les envoie au contrôleur maître.

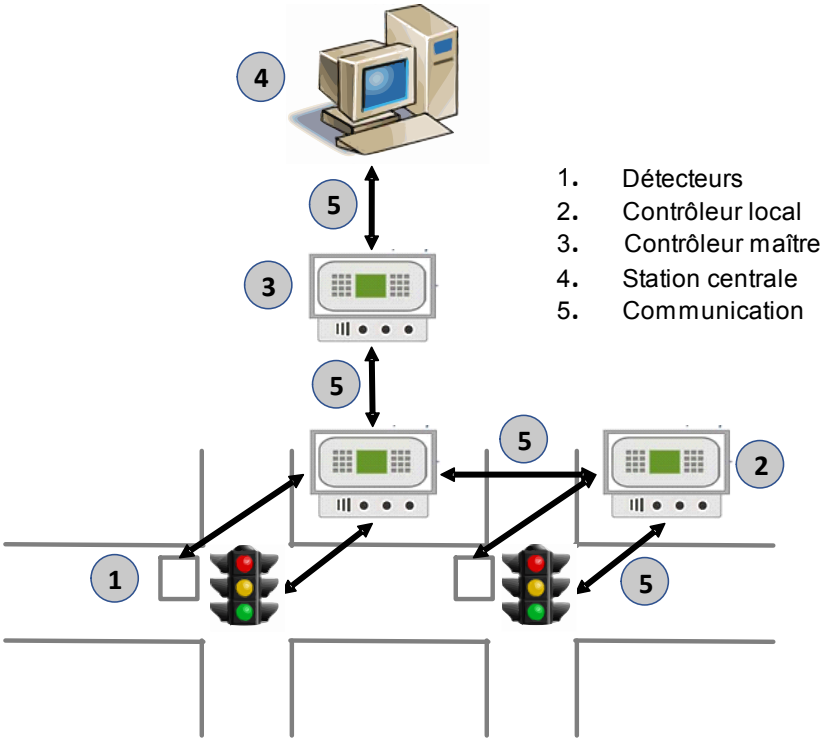


Figure 2.4 : Composants d'un système répartis sur trois niveaux (adaptée de [25])

La communication permet l'échange bidirectionnel d'information entre les composants du système. Elle est implémentée en utilisant différents moyens. La fibre optique, le câble coaxial et les lignes téléphoniques fixes (propriétaires ou louées) sont quelques-uns de ces moyens. Parmi ceux-ci, les lignes téléphoniques fixes ont été les plus populaires. Cependant, avec des avancements de la technologie, il y a une tendance à utiliser de plus en plus la communication sans fil. En plus d'utiliser les moyens traditionnels de transmission d'information sans fil, tels que les micro-ondes et la radiofréquence, les concepteurs des systèmes évaluent d'autres approches. Par exemple, les réseaux cellulaires, la transmission par satellite et la radiocommunication tant par paquets qu'à large spectre, sont des approches considérées [30].

2.5.2 Systèmes répartis en deux niveaux

Contrairement aux systèmes répartis sur trois niveaux, il n'y a pas de contrôleurs maîtres dans les systèmes répartis sur deux niveaux. En conséquence, toutes les fonctions du contrôleur maître sont exécutées par le CGT. Par contre, les fonctions des contrôleurs de feux de circulation restent les mêmes que celles des contrôleurs locaux des systèmes répartis sur trois niveaux.

2.5.3 Systèmes centralisés

L'architecture des systèmes centralisés n'inclut pas le contrôleur maître, mais elle incorpore une unité de communication à distance (« Remote Communication Unit ») pour établir la communication entre le CGT et les contrôleurs de feux. Cette unité sert principalement à faire correspondre les interfaces et les protocoles des contrôleurs de feux avec ceux du CGT.

Dans cette architecture, le CGT traite et filtre les données recueillies par les détecteurs, calcule les plans de feux et les sélectionne en fonction des conditions du trafic. De plus, le CGT contrôle directement la durée des phases de chaque feu de circulation. Le CGT envoie des commandes aux contrôleurs de feux pour terminer chaque phase. Il s'appuie sur l'information des plans de feux pour déterminer le moment précis pour terminer les phases [31].

Pour leur part, les contrôleurs de feux transmettent au CGT l'information récoltée par les détecteurs et aussi l'état (actif) des intervalles de feu vert. Ils stockent aussi une copie des plans de feux et commutent les feux en fonctions des commandes reçues du CGT. Ils se servent des plans de feux pour implémenter la coordination basée sur la planification horaire, en cas de pannes de la communication ou du CGT.

2.6 Conclusion

Dans ce chapitre, nous avons présenté des notions de la régulation du trafic routier afin de faciliter la compréhension des prochains chapitres de ce mémoire. Comme il a été vu, les feux de circulation attribuent de façon automatique le droit de passage aux différents flux convergeant aux intersections afin de garantir la sécurité des usagers et d'améliorer la fluidité de la circulation. L'information concernant l'ordre de passage de chaque flux dans le carrefour et le temps qui leur est attribué pour le faire est contenue dans le plan de feu, ce qui est utilisé par les contrôleurs de feux pour commuter les feux de signalisation. Pour réguler le trafic aux carrefours, les contrôleurs des feux peuvent s'appuyer sur l'information concernant la présence des véhicules saisie par des détecteurs ou sur l'information historique des conditions du trafic. Ils peuvent aussi réguler le trafic aux intersections de façon isolée, sans considérer les carrefours à proximité, ou en coordination avec des carrefours à feux adjacents, afin de promouvoir la circulation des pelotons de véhicules se déplaçant sur des corridors ou de petits réseaux routiers. La coordination peut être implémentée en utilisant différentes techniques, mais indépendamment de la technique utilisée, les paramètres

des plans des feux de tous les carrefours à feux du système doivent être calculés soigneusement pour accomplir les objectifs de régulation tant localement à chaque carrefour que globalement dans l'ensemble (corridor ou réseau).

Dans le cadre de notre recherche, il est indispensable d'avoir une bonne connaissance du fonctionnement, des architectures et des composants des systèmes de contrôle de trafic routier, mais aussi il est nécessaire de connaitre les vulnérabilités qui les rendent susceptibles à des attaques informatiques aussi que les attaques et menaces informatiques auxquelles ils sont exposés. Étant donné que les systèmes de contrôle de trafic routier sont aussi des systèmes de contrôle industriels, dans le prochain chapitre nous aborderons les aspects de la sécurité des systèmes de contrôle industriels, et montrerons des travaux antérieurs qui ont été faits dans le cadre de l'évaluation de la sécurité informatique des systèmes de contrôle industriels et des systèmes de contrôle de trafic routier.

CHAPITRE 3 REVUE DE LITTÉRATURE

Dans le chapitre précédent, nous avons présenté les notions basiques de la régulation du trafic routier afin de faciliter la compréhension du contenu de ce mémoire. Pour sa part, ce chapitre visera à présenter un portrait de la sécurité informatique des systèmes de contrôle industriels actuels, incluant les systèmes de contrôle de trafic routier.

Nous commencerons par les notions des systèmes de contrôle industriels, incluant leurs architectures et composants. Ensuite, nous expliquerons les raisons pour lesquelles les systèmes de contrôle industriels actuels sont plus vulnérables qu'auparavant à subir des attaques informatiques. Nous continuerons avec des notions de la sécurité informatique en expliquant les objectifs de la sécurité, et les attaques et menaces informatiques auxquelles les systèmes de contrôle industriels actuels sont exposés. Après nous décrirons de vrais cas d'attaques informatiques qui ont été lancées contre des systèmes contrôlant des infrastructures critiques aux différentes parties du monde. Finalement, nous présenterons une sélection de travaux portant sur l'usage de la co-simulation pour évaluer la sécurité informatique des systèmes de contrôle industriels et des évaluations de la sécurité des systèmes de contrôle du trafic.

3.1 Systèmes de contrôle

Les systèmes de contrôle sont des systèmes basés sur des ordinateurs destinés à surveiller et contrôler des processus physiques. Ils sont intégrés par des boucles de contrôle contenant capteurs et actuateurs qui interagissent avec le processus physique, les interfaces des opérateurs et des applications pour le diagnostic et la maintenance à distance du système [32]. De façon générale, ils collectent l'information du processus et implémentent des actions de contrôle en suivant une logique préétablie et en utilisant l'information collectée. En conséquence, le processus physique agit d'une manière déterminée (souhaitable) au fil du temps. De nos jours, les systèmes de contrôle intègrent les technologies de l'information (qui traitent les données recueillies) avec les technologies d'opération (qui contrôlent les processus) et les technologies de la communication (qui permettent l'échange d'information). Ces systèmes sont utilisés dans des domaines très variés, tels que la distribution d'eau, la production et le transport d'énergie, la production de pétrole et de gaz, le transport de biens et personnes, la gestion du trafic routier, la santé et la fabrication, entre

autres. La Figure 3.1 montre un schéma général des composants et du fonctionnement d'un système de contrôle de processus.

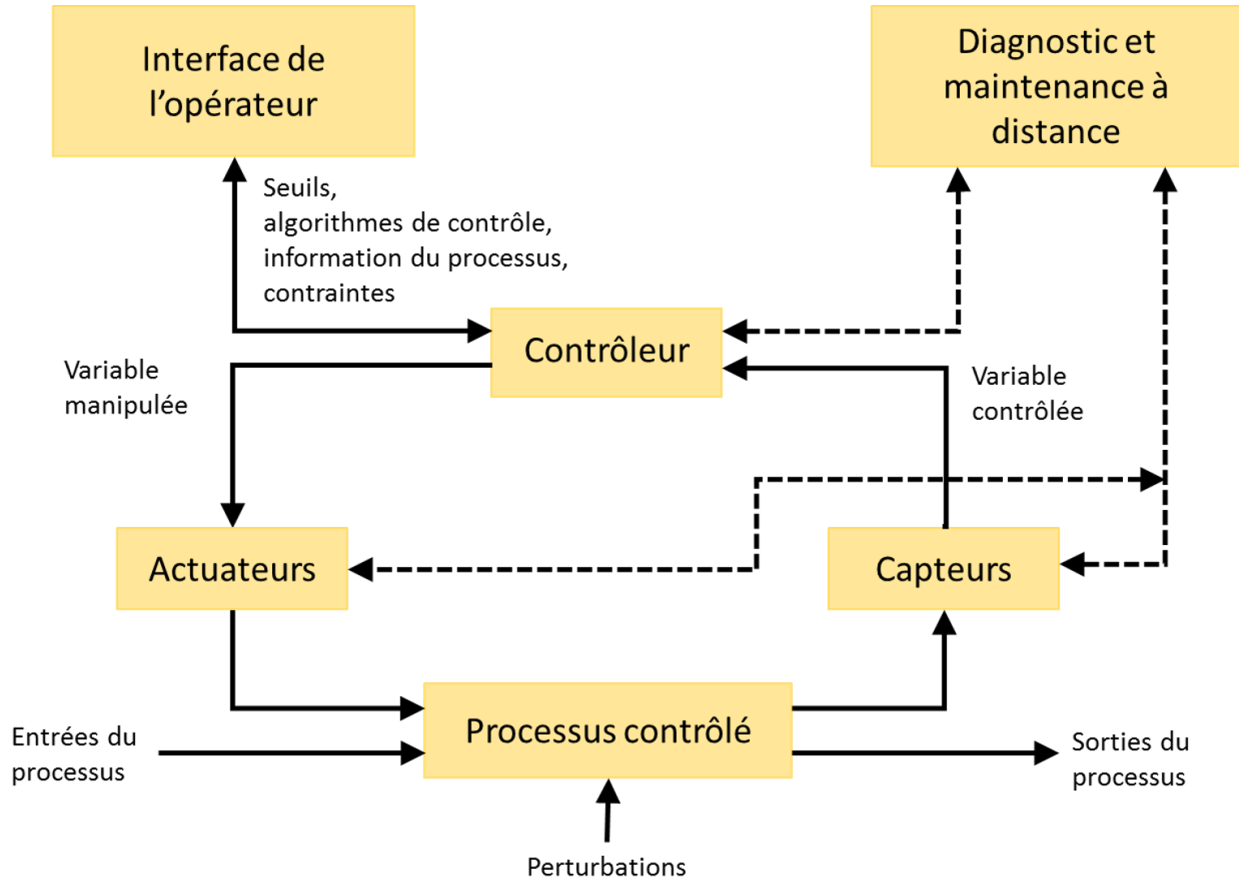


Figure 3.1 : Schéma général d'un système de contrôle de processus (adapté de [33])

À la différence des systèmes de l'information, dont la tâche principale est le traitement, le stockage et la transmission de données, les systèmes de contrôle surveillent l'état des processus et commandent des dispositifs physiques, tels qu'interrupteurs, valves, moteurs, etc., pour maintenir l'état du processus dans la plage de fonctionnement désirée. Pannes ou perturbations dans l'opération des systèmes de contrôle peuvent entraîner des impacts multiples et importants, allant des pertes économiques au dommage à la propriété et aux personnes [8].

Les systèmes contrôlent les processus physiques soit en tenant compte de la réaction du processus (« feedback ») ou pas. Les systèmes qui ne prennent pas en compte la réaction du processus sont appelés systèmes en boucle ouverte. Ils n'exercent aucune action de contrôle pour compenser les changements dans l'état du processus. Par contre, les systèmes en boucle fermée, comme celui montré à la Figure 3.1, considèrent la réaction du processus. Ils s'appuient sur quatre fonctions

primordiales pour maintenir le processus dans l'état désiré : la mesure, la comparaison, le calcul et la correction. Ils mesurent les valeurs des paramètres de contrôle saisies par des capteurs, les comparent avec les valeurs idéales (seuils), calculent la déviation entre les deux valeurs (erreur) et commandent les dispositifs de contrôle final (actuateurs) pour corriger cette erreur [34]. L'élément responsable de faire la comparaison, le calcul et l'identification des actions de contrôle à implémenter est le contrôleur. Dans la plupart des systèmes de contrôle automatisés, les contrôleurs sont des ordinateurs qui exécutent des logiciels spécialisés adaptés au processus à contrôler [35].

Selon leur application, les systèmes de contrôle sont aussi appelés systèmes de contrôle de processus, systèmes de contrôle industriels ou systèmes cyber-physiques [36]. Les systèmes de contrôle de processus sont généralement associés aux processus qui se déroulent à l'intérieur des usines ou dans des espaces confinés, comme les industries manufacturières. Par contre, les systèmes de contrôle industriels sont associés aux processus et infrastructures critiques dispersés géographiquement (souvent sur des milliers de kilomètres carrés), tels que les systèmes de distribution et traitement de l'eau, de distribution de pétrole et de gaz, le réseau électrique et les systèmes de transports, entre autres [33].

Le terme de système de contrôle industriel est attribué de façon générale à différents types de systèmes et leur instrumentation associée, utilisés pour contrôler et automatiser des processus industriels. Les systèmes SCADA (acronyme de « Supervisory Control and Data Acquisition ») et les systèmes de contrôle distribués (« Distributed Control Systems », DCS) sont deux types de systèmes de contrôle industriels. Les contrôleurs logiques programmables (« Programable Logic Controler », PLC), les unités de télécommande à distance (« Remote Terminal Unit », RTU) et les dispositifs électroniques intelligents (« Intelligent Electronic Devices », IED), entre autres, constituent l'instrumentation des systèmes de contrôle industriels [37] [38].

Les systèmes SCADA et les DCS se différencient par la façon de contrôler le processus : les systèmes SCADA s'appuient sur le contrôle centralisé tandis que les DCS s'appuient sur le contrôle distribué. Dans les systèmes SCADA, la surveillance et le contrôle s'exécutent à une station centrale, aussi appelée « Master Terminal Unit », (MTU). La MTU reçoit et traite toute l'information collectée du processus et exerce les actions de contrôle (émission de commandes). Par contre, les DCS sont composés de plusieurs sous-systèmes contrôlés qui communiquent avec une station centrale. Chaque sous-système est géré par un contrôleur local, soit RTU, PLC et/ou

IED. La station centrale collecte l'information de tous les sous-systèmes (aux fins de surveillance), calcule les seuils de toutes les variables contrôlées et les envoie à chaque contrôleur local. De leur côté, les contrôleurs locaux commandent les actuateurs en fonction des seuils reçus et de l'information collectée par les capteurs [33].

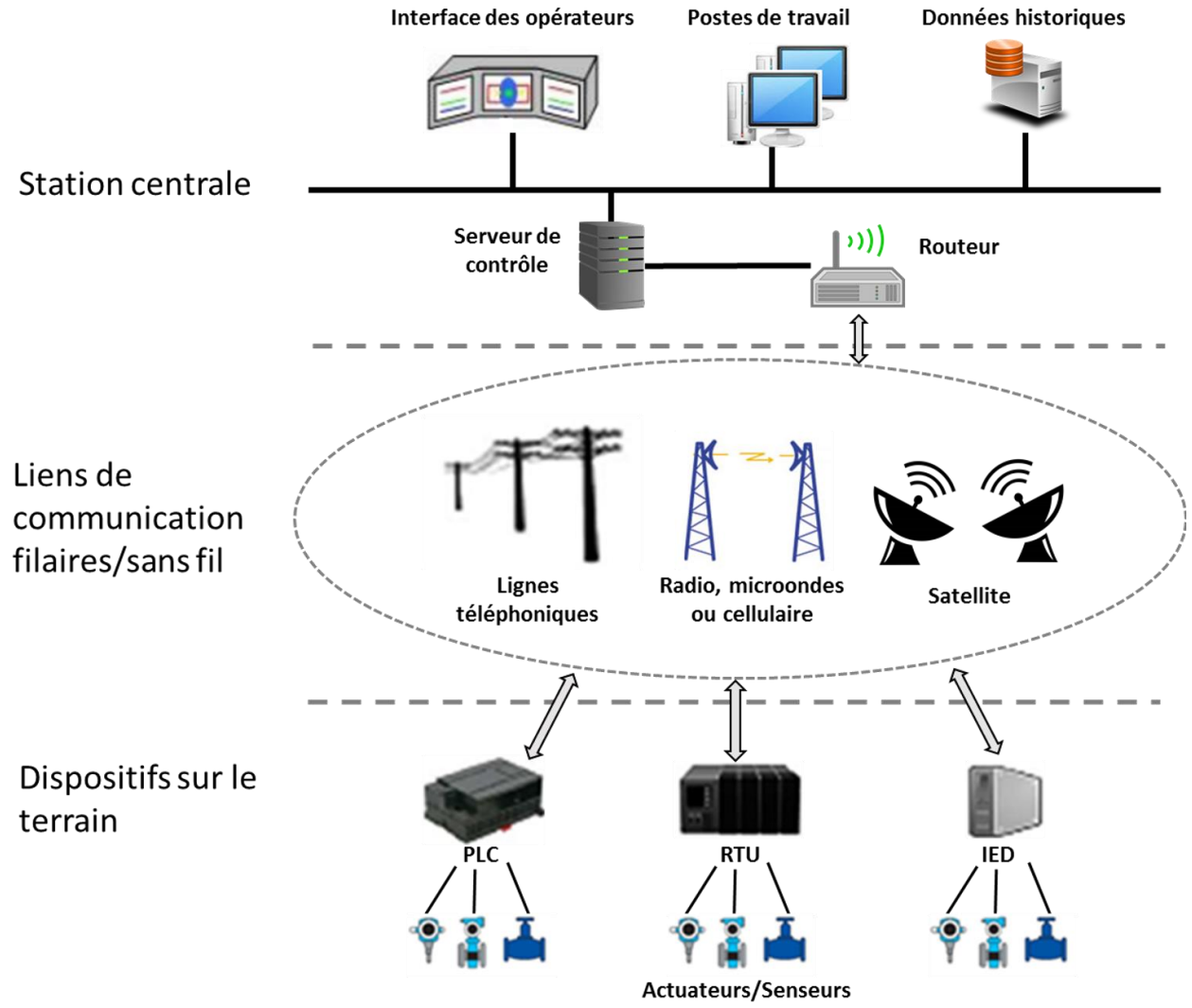


Figure 3.2 : Architecture typique d'un système de contrôle industriel SCADA (adapté de [39])

La Figure 3.2 montre l'architecture typique d'un système SCADA. On y distingue trois groupes fonctionnels : les dispositifs sur le terrain, les liens de communication et la station centrale. Les dispositifs sur le terrain (RTU, PLC et/ou IED) collectent l'information sur le processus, obtenue par les capteurs, la convertissent et la transmettent à la station centrale en se servant des liens de communication. Ils dirigent aussi les commandes émises par la station centrale vers les actuateurs du processus. Pour sa part, la station centrale traite l'information du processus, l'enregistre et

l'affiche sur l'interface des opérateurs. De ce fait, les opérateurs peuvent surveiller et contrôler tout le système presque en temps réel. Les actions de contrôle sont générées à la station centrale, soit par l'exécution d'une logique automatique ou par l'opérateur [39].

De nos jours, des éléments de chaque groupe fonctionnel mentionné dans le paragraphe antérieur possèdent vulnérabilités informatiques. En conséquence, il est possible que des individus malveillants accèdent aux systèmes de contrôle et les manipulent. La section suivante présente les vulnérabilités informatiques les plus communes associées aux systèmes de contrôle actuels.

3.2 Vulnérabilités informatiques des systèmes de contrôle actuels

La plupart des auteurs des travaux portant sur la sécurité informatique des systèmes de contrôle industriels conviennent qu'aujourd'hui ces systèmes sont plus susceptibles qu'auparavant de subir des attaques informatiques. Lesdits auteurs aussi attribuent le risque élevé des attaques à la croissance du nombre de vulnérabilités informatiques détectées dans les dernières années et au fait que ces vulnérabilités sont de plus en plus vulgarisées et accessibles par un nombre croissant d'adversaires motivés et hautement qualifiés [40]. Dans le rapport sur les menaces à la sécurité de l'Internet de l'année 2016 [41], Symantec montre que le nombre de vulnérabilités informatiques des systèmes de contrôle industriels est monté en flèche en 2015 (Figure 3.3) et que ces vulnérabilités sont liées à une variété de fabricants et dispositifs utilisés dans les systèmes de contrôle.

Les vulnérabilités informatiques des systèmes de contrôle peuvent se produire dans le matériel, le micrologiciel (« firmware ») et les logiciels des composants utilisés. Les sources de vulnérabilités sont variées, allant des défauts de conception et des failles de développement, à des mauvaises configurations, des politiques de maintenance et d'administration inadéquates et des faiblesses architecturales des systèmes, entre autres [33]. Dans cette section nous présentons les causes qui rendent les systèmes de contrôle actuels vulnérables aux attaques informatiques. Ce sont les causes les plus fréquentes identifiées dans la littérature.

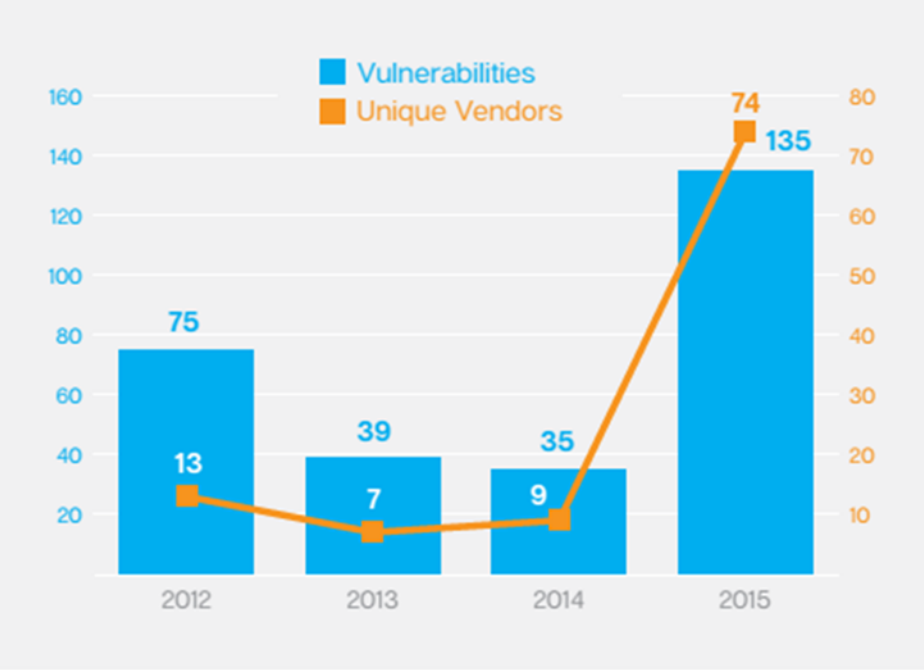


Figure 3.3 : Vulnérabilités découvertes dans les systèmes de contrôle industriels [41]

3.2.1 Usage de protocoles de communication non sécurisés

La plupart des protocoles de communication utilisés dans les réseaux industriels ont été conçus pour travailler dans environnements isolés et la sécurité n'a pas été considérée pendant leur conception [33] [42] [43]. En conséquence, ils ne possèdent pas des mécanismes d'authentification (qui identifient l'émetteur des messages), de chiffrement (qui assurent que le contenu des messages est compréhensible seulement pour les personnes autorisées) ou d'intégrité de l'information (qui empêchent de modifier le contenu des messages). De plus, ces protocoles ont été originalement développés pour des communications séries, mais de nos jours la majorité d'eux ont été intégrés à la suite des protocoles TCP/IP et ils ont hérité les vulnérabilités informatiques de ce protocole-ci [43].

Herrero et López [44], Wanying, Weimin, Surong et Yan [45] et Jakaboczki et Adamko [46], ont évalué la sécurité informatique de huit protocoles de communication communément utilisés dans les réseaux de contrôle de processus industriels. Ils ont trouvé que seulement deux des protocoles évalués possèdent mécanismes d'authentification et de chiffrement. En raison de ces résultats, ils manifestent qu'un adversaire qui accède au réseau de communication peut lire le contenu des

messages échangés et, en ayant connaissance du système et du protocole, il peut aussi injecter des messages valides dans le réseau et manipuler le comportement du système.

Cerrudo [14] a bien démontré la véracité de cette affirmation en réussissant à manipuler l'état des feux de circulation à Seattle, Washington, D. C. et New York en modifiant l'information envoyée par les capteurs installés dans la chaussée aux contrôleurs de feux de circulation. Pour ce faire, il a capturé des messages échangés dans le réseau, leur a appliqué l'ingénierie inverse pour apprendre le fonctionnement du protocole de communication et a modifié l'information envoyée par des capteurs aux feux de circulation.

Ghena *et al.* [13] et Cerrudo [14] ont démontré que des composants des systèmes actuels de régulation de la circulation manquent de mécanismes et de politiques de sécurité adéquats pour se protéger d'attaques informatiques. Les résultats de leurs travaux mettent en avant : 1) l'usage de faibles mécanismes de contrôle, voire d'aucun mécanisme, pour accéder aux dispositifs critiques du système, tels que les contrôleurs de feux de circulation, les points d'accès et les commutateurs du réseau de communication, 2) le manque de chiffrement et d'authentification des communications et 3) le manque de signature du micrologiciel. Dans ces conditions, ils ont inséré des messages dans le réseau de contrôle et ont manipulé les feux de circulation. Il a suffi que les messages soient bien encodés pour que les contrôleurs les considèrent comme étant valides.

En plus des protocoles de communication dédiés au contrôle, les systèmes de contrôle actuels utilisent aussi des protocoles de communication et services d'accès à distance, tels que FTP (« File Transfer Protocol »), Telnet et rsh (« remote shell ») qui ne sont pas sécurisés. Cela signifie que des informations critiques, comme les identifiants utilisateurs, mots de passe et même commandes de contrôle, sont transmises en texte clair. En conséquence, un adversaire pouvant intercepter les messages échangés, peut lire leur contenu, prendre connaissance de l'information envoyée et l'utiliser ultérieurement contre le système [32] [47].

3.2.2 Multiples points d'entrée et d'échec

Comme nous avons expliqué auparavant, les systèmes de contrôle industriels se composent de dispositifs de mesure et commande dispersés géographiquement qui se connectent à une station centrale à travers d'un réseau de communication. En générale, le réseau et les ordinateurs à la station centrale sont munis de mécanismes de sécurité pour les protéger des attaques informatiques.

Par contre, des dispositifs sur le terrain (capteurs, actuateurs, PLCs, IEDs, etc.) ne sont pas adéquatement protégés et possèdent des vulnérabilités exploitables par des adversaires [48].

D'un autre côté, les réseaux de communication modernes emploient diverses technologies, telles que les communications sans fil, les communications cellulaires, le Bluetooh et l'Internet, ce qui fournit des multiples points d'accès qui peuvent être exploités par les attaquants.

3.2.3 Interconnexion avec d'autres systèmes et réseaux

Auparavant, les systèmes de contrôle opéraient de façon isolée. Cela signifie qu'aucune connexion avec d'autres systèmes ou réseaux n'était permise. Pour attaquer ses systèmes il fallait se connecter physiquement à ses composants. Mais le besoin de décisions appropriées, afin de maintenir la rentabilité des entreprises et leur position dans le marché, a mené à la substitution des anciens systèmes isolés par systèmes intégrés qui connectent les différents systèmes automatisés entre eux et avec les systèmes d'information des bureaux [49]. Une telle interconnexion s'avère nécessaire pour les gestionnaires d'affaires, car ils ont besoin d'accéder à l'information précise et actualisée du système et de l'état du processus afin de prendre des décisions sur la gestion de l'entreprise.

Au début, les protocoles et mécanismes de communication propriétaires et spécialisés étaient favorisés pour implémenter ces interconnexions. Cependant, aujourd'hui ils ont été remplacés par des protocoles de communication et des technologies ouvertes et standardisées, et même l'Internet. En conséquence, les systèmes de contrôle actuels sont potentiellement accessibles depuis l'Internet et exposés aux mêmes vulnérabilités informatiques des systèmes de technologie de l'information [50]. McLaughlin *et al.* [39] affirment qu'au début des années 2000, la majorité des attaques informatiques contre les systèmes de contrôle étaient exécutées par des attaquants internes aux entreprises, mais que lors que les systèmes ont été connectés à l'Internet, les attaques exécutées par des sources externes aux entreprises ont subi une augmentation importante.

3.2.4 L'usage de produits informatiques standards

Afin de favoriser l'intégration des différentes technologies et de réduire les coûts d'achat et d'opération, les nouvelles solutions d'automatisation et contrôle industriels sont basées sur les systèmes embarqués et les plateformes informatiques standards, voire des logiciels et matériels

COTS[1] [43]. Cela signifie qu'un même dispositif, par exemple un modem ou un routeur, peut être utilisé tant dans un réseau de bureau que dans un réseau de contrôle. Donc, un adversaire avec des connaissances de son opération et sa configuration peut s'en servir pour attaquer le réseau de contrôle [49].

D'un autre côté, des produits informatiques standards possèdent des vulnérabilités connues et de faibles mécanismes de sécurité pour se protéger d'attaques informatiques. À titre d'exemple, Cui et Stolfo [51] ont fait une analyse quantitative des faiblesses informatiques des dispositifs embarqués accessibles depuis l'Internet. D'abord, ils se sont servis de l'outil de balayage de ports « nmap » pour construire un scanner d'informations d'identification par défaut. Ensuite, ils l'ont utilisé pour accéder aux dispositifs connectés à l'Internet qui utilisaient les informations d'identifications par défaut les plus connues. Comme résultat, ils ont accédé à 540 000 dispositifs, ce qui représente environ 13% du total des produits embarqués détectés au cours de l'analyse. Ces dispositifs appartiennent aux catégories suivantes : appareils de bureau, dispositifs de réseaux domestiques, dispositifs de gestion d'énergie des centres informatiques (« data centers »), appareils de sécurité de réseaux, modems des fournisseurs de service d'Internet, systèmes de surveillance par caméra de vidéo, etc. Cette analyse met en avant que l'usage des informations d'identification par défaut est une pratique répandue qui dégrade la sécurité informatique des systèmes dans plusieurs domaines. À titre d'exemple, Ghena *et al*. [13] ont fait la même constatation lors de l'évaluation de la sécurité informatique des éléments intégrés à un système de contrôle du trafic routier actuellement en service à Michigan.

3.2.5 L'usage de systèmes patrimoniaux (« legacy systems »)

Les premiers systèmes de contrôle ont été conçus en accordant plus d'importance à la disponibilité et la fiabilité qu'à la sécurité. À l'époque, ce manque de sécurité n'entraînait pas des problèmes majeurs, car les systèmes opéraient généralement dans des environnements isolés et utilisaient des logiciels, matériels et protocoles de communication propriétaires. Au cours des années, de nouvelles technologies sont apparues et ces systèmes sont devenus désuets. En dépit de cette

[1] COTS est l'abréviation de « Commercial off-the-shelf ». Cette terminologie fait référence aux produits informatiques qui ont été fabriqués en série pour l'usage général et pas pour une application spécifique [96].

situation, de nombreux systèmes anciens sont toujours en service, car les remplacer entraîne des coûts importants, que les usagers préfèrent en éviter, ou des impacts négatifs sur le fonctionnement du système [52]. En conséquence, les systèmes de contrôle actuels sont intégrés avec de vieux composants dont leurs vulnérabilités informatiques sont connues et exploitables.

De plus, la majorité des systèmes hérités du passé qui restent en service aujourd'hui ne bénéficie plus du support technique de leurs fabricants. En ce qui a trait aux produits logiciels, tels que les systèmes d'exploitation, les correctifs (« patchs ») aux vulnérabilités détectées ne sont plus fournis. Or, même si les fabricants continuent à fournir les correctifs, la nature des processus contrôlés exige que les systèmes fonctionnent de façon ininterrompue, ce qui rend difficiles et peu fréquentes les arrêts pour installer les correctifs. À titre d'exemple, lors d'une évaluation de la sécurité d'un système contrôlant une centrale de production d'énergie, Masera, Forvino et Leszczyna [53] ont détecté que la plupart des serveurs du réseau SCADA utilisaient systèmes d'exploitation anciens et dépourvus des correctifs les plus récents. En plus, les résultats de l'enquête *2017 Security Patching is Hard* [52] révèlent que 72 % des participants déclarent de ne pas appliquer des correctifs logiciels, car ils craignent que ceux-ci ne puissent entrainer des pannes de systèmes.

D'un autre côté, intégrer des outils de sécurité informatique standards (détection des intrusions, balayage des ports, services de chiffrement, etc.) dans un système de contrôle intégrant d'anciennes technologies, peut augmenter la latence du réseau ou produire des erreurs opérationnelles dans le système menant à son arrêt partiel ou total [32].

3.2.6 La sécurité par l'obscurité (« security by obscurity »)

Une autre raison pour laquelle les premiers systèmes de contrôle industriels étaient moins vulnérables aux cyberattaques était l'accès à l'information. Auparavant, l'accès à l'information vitale pour opérer et configurer les systèmes de contrôle était présumée restreinte aux vendeurs et usagers. Cependant, avec la croissance de l'automatisation des processus industriels les mêmes solutions en automatisation sont utilisées par les entreprises dans le monde entier, ce qui rend l'information technique sur les systèmes de plus en plus disponible [49]. De plus, les informations détaillées sur les dispositifs et les applications utilisés dans les systèmes de contrôle sont disponibles sur l'Internet. Par exemple, Zetter [54] note l'existence sur l'Internet du mot de passe pour accéder à la base de données du système SCADA Simantic WinCC de Siemens. Le mot de passe a été intégré en hard code au système pendant sa conception et il est disponible sur l'Internet

depuis 2008. Byres [55] affirme que cette vulnérabilité a été exploitée par le ver Stuxnet, qui a été utilisé pour attaquer une usine d'enrichissement d'uranium en Iran, entre autres installations industriels. Zetter a dénoncé aussi la publication sur l'Internet d'un code pour exploiter des vulnérabilités détectées dans certains systèmes SCADA utilisés dans certaines installations de gestion de gaz, de pétrole et d'eau [56]. Le code permet d'exécuter des attaques du type de débordement de tampon (« buffer-overflow »), de déni de service, d'injection de paquets, et même d'exécution à distance de code malveillant [32]. Pour sa part, Mills [57] affirme qu'en utilisant le moteur de recherche de Google il est possible de trouver des équipements des infrastructures critiques qui peuvent être commandés à distance depuis l'Internet.

Luallen [58] a démontré à quel point l'information disponible sur l'Internet attente à la sécurité des systèmes de contrôle actuels. Un groupe de ces étudiants en sécurité à l'Université DePaul (Illinois) se sont servis des outils « Open Source Intelligence[2] » (OSINT) pour chercher sur l'Internet des informations concernant les vulnérabilités et les exploits permettant d'attaquer des systèmes de contrôle couramment en service. Comme résultat, les étudiants ont trouvé des informations détaillées concernant : 1) la configuration, les composants, l'architecture et les protocoles de communication utilisés par les systèmes ciblés, 2) les vulnérabilités et vecteurs d'attaques déjà identifiés, et 3) les outils développés pour exploiter les vulnérabilités connues. Une telle information pourrait être utilisée par un adversaire pour exécuter de vraies attaques contre les systèmes étudiés.

3.3 Notions de sécurité informatique

Cette section est consacrée à présenter les objectifs fondamentaux de la sécurité informatique des systèmes de contrôle industriels et à décrire les caractéristiques des attaques informatiques et des logiciels malveillants qui peuvent être utilisés contre ces systèmes. Cela facilitera la compréhension de l'information présentée dans les sections suivantes de ce chapitre.

---

[2] Open source intelligence fait référence à l'analyse d'information récoltée, à partir des sources publiques ou ouvertes, qui est utilisée dans le contexte de l'intelligence. Les outils OSINT permettent de collecter autant d'informations que possible concernant à une cible déterminée.

3.3.1 Objectifs de la sécurité

La sécurité informatique fait référence à la protection de l'information et des ressources tant matérielles que logicielles d'un système. Dans le contexte des systèmes de contrôle industriels, la sécurité informatique fait référence non seulement à la protection de l'information stockée dans le système, mais aussi à la protection de l'information lors de sa transmission entre deux points du système, c'est-à-dire la sécurité des réseaux [59]. Cette protection signifie empêcher l'accès des entités non autorisées aux composants du système afin d'éviter que l'information soit volée ou endommagée et que le système soit indument manipulé [60]. Pour ce faire, la sécurité informatique de systèmes de contrôle s'appuie sur certains objectifs de sécurité, qui sont : la confidentialité, l'intégrité, la disponibilité, l'authentification, la non-répudiation et le contrôle d'accès [49] [61]. La confidentialité vise à garantir que seulement les entités autorisées peuvent accéder à l'information; l'intégrité vise à éviter la destruction ou modification de l'information par des entités non autorisées; la disponibilité vise à rendre l'information et les services disponibles pour tous les usagers en tout temps; l'authentification assure que les entités sont ce qu'elles prétendent être; la non-répudiation vise à associer chaque entité avec ses actions afin que l'entité ne puisse pas nier ou rejeter les avoir faites; finalement, le control d'accès vise à interdire l'accès des entités illégitimes aux ressources du système [49] [62].

Dans les systèmes de technologie de l'information, la priorité accordée aux objectifs de la sécurité est : confidentialité, intégrité et disponibilité. C'est qui est appelé la triade CIA (par les initiales en anglais des objectifs). Cependant, dans les systèmes de contrôle industriels, cet ordre varie, en attribuant plus de priorité à la disponibilité, suivie par l'intégrité et finalement la confidentialité. Cet ordre dérive de la nature des processus contrôlés, qui exigent surveillance et contrôle continus en temps réel.

3.3.2 Attaques et menaces informatiques

La violation intentionnelle d'au moins l'un des critères de sécurité constitue une attaque informatique [49]. Les attaques sont objet de plusieurs classifications. Par exemple, selon l'intention de l'attaque, les attaques peuvent être passives ou actives. Les attaques passives ont pour objectif de connaître l'information transmise entre deux points du réseau, mais elles n'exécutent aucune action contre le système. Par contre, les attaques actives ont pour objectif

d'altérer les ressources ou le comportement du système [63]. Selon la nature de l'attaquant, les attaques peuvent être internes ou externes. Les attaques internes sont exécutées par des personnes à l'intérieur de l'organisation tandis que les attaques externes sont exécutées par des personnes à l'extérieur. Selon la nature des victimes, les attaques peuvent être aléatoires ou ciblées. Dans les attaques aléatoires, l'attaquant vise à exploiter une vulnérabilité particulière et les victimes sont les systèmes ou dispositifs qui possèdent cette vulnérabilité. Par contre, dans les attaques ciblées, les victimes sont choisies et étudiées avant l'attaque. Dans ce cas, les adversaires exécutent d'abord une étape de reconnaissance du système visant à collecter autant d'informations que possible. Ultérieurement, ils élaborent leur stratégie d'attaque en fonction de l'information collectée et avec le but d'endommager le processus physique. Ce type d'attaque est généralement associé à l'espionnage industriel et au terrorisme [48].

Voici une description des caractéristiques des attaques informatiques les plus communes (tiré de [63] [64]) :

- Attaque d'écoute (« eavesdropping » ou « sniffing »). C'est une attaque passive qui attente à la confidentialité de l'information. Le but de l'attaquant est de lire le contenu des messages transmis. Il utilise des outils logiciels ou matériels pour intercepter et examiner le contenu des messages échangés sur le réseau.
- Attaque d'analyse de trafic. C'est un autre type d'attaque passive. Dans ce cas, l'adversaire peut ne pas lire le contenu des messages échangés (si chiffrés), mais il peut obtenir des informations importantes, telle que les adresses IP des serveurs, et deviner la nature des fonctions des serveurs, à partir de l'analyse de la communication dans le réseau.
- Attaques de déni de service (« denial of service »), ou attaques de saturation. C'est une attaque active qui attente à la disponibilité. L'adversaire vise à empêcher que les usagers accèdent à un serveur ou à un réseau. L'une des façons de le faire est en saturant le serveur avec une très grande quantité de requêtes afin que le serveur ne puisse pas traiter les requêtes provenant des usagers légitimes.
- Attaque de rejeu (« replay attack »). C'est une attaque active qui attente à l'intégrité. Dans ce cas, l'adversaire capture un message transmis entre deux dispositifs, le garde et le retransmet ultérieurement afin de produire un effet sur le système.

- Attaque de mascarade, ou injection de paquets. C'est une attaque active qui attente à l'authenticité. Dans ce type d'attaque, l'adversaire utilise l'information contenue dans des messages capturés pour prétendre être une autre entité. En se servant de cette information, l'adversaire construit des faux messages et les insère dans le réseau comme s'ils étaient légitimes.
- Attaque de l'homme au milieu (« man-in-the-middle »). C'est une attaque active qui attente à l'intégrité de l'information. Dans ces attaques, l'adversaire intercepte un message envoyé de A à B avant qu'il soit livré à B. Ensuite, l'adversaire modifie le contenu du message et l'envoie à B comme si le message provenait de A.
- Attaque par usurpation d'adresse IP (« IP spoofing »). C'est une attaque active qui attente à la non-répudiation. Dans ce cas, l'adversaire attribue à sa machine (ordinateur) une fausse adresse IP afin de se faire passer par une autre machine.
- Ingénierie sociale. Cette terminologie fait référence à des pratiques de manipulation psychologique avec le but d'arnaquer quelqu'un. Cette pratique s'appuie sur l'exploitation des faiblesses psychologiques, sociales et organisationnelles afin d'obtenir quelque chose de la victime, généralement de l'argent ou de l'information. L'attaquant se sert de son charisme pour abouser de la confiance et de la crédulité des victimes [65].
- Attaque par intrusion. C'est une attaque active qui attente au contrôle d'accès. L'attaquant accède au système en se servant des informations d'utilisateurs qui ont été obtenues soit des messages interceptés, ou en utilisant des méthodes d'ingénierie sociale, ou en utilisant des techniques pour deviner le mot de passe d'un utilisateur légitime.
- Hameçonnage (« phishing »). L'adversaire se fait passer par une entité légitime, tel que l'administrateur du système, et demande aux victimes de fournir leurs informations personnelles en raison d'un motif quelconque, tel qu'une mise à niveau du système, une mise à jour de la base de données, un plantage du système, etc. [61].
- Harponnage (« spear phishing »). Dans cette attaque, l'adversaire envoie des courriels aux victimes ciblées et les fait passer par des courriels envoyés par des sources fiables ou par des amis. Le corps du courriel contient des informations sur la victime, qui a été obtenue à l'avance à partir des informations disponibles publiquement ou d'autres attaques, et qui sert

à la convaincre de l'authenticité de l'émetteur. L'adversaire utilise des prétextes pour encourager les victimes à lire le contenu d'un fichier attaché au message. Une fois le fichier est ouvert, un logiciel malveillant s'installe dans les machines des victimes. Ultérieurement, l'adversaire se sert du logiciel installé pour accéder aux machines.

Pour sa part, les menaces informatiques font référence aux logiciels malveillants, c'est-à-dire, les logiciels qui s'exécutent à l'insu des usagers et qui visent à produire des impacts négatifs sur le système. Ils sont conçus dans le but d'accéder à des informations critiques, de contourner les mécanismes de contrôle d'accès ou de modifier le fonctionnement du système, entre autres. Voici la description des types de logiciels malveillants les plus répandus (tirée de [49] [63] [64] [66]):

- Virus informatique. C'est un logiciel qui a la propriété de se reproduire de façon autonome. Il fait partie d'un code et lorsque ce code s'exécute, le virus se reproduit et s'ajoute aux fichiers se trouvant dans la machine. Puis, il utilise les fichiers infectés pour se propager à d'autres machines dans le réseau. Les virus visent à nuire ou perturber le fonctionnement des ordinateurs.

- Ver informatique (« worm »). Similairement aux virus, les vers informatiques se reproduisent de façon autonome, mais ils n'utilisent pas de fichiers infectés pour se propager. Leur propagation s'appuie sur la détection et l'exploitation de vulnérabilités dans la machine victime. Les vers sont conçus avec un objectif déterminé, soit pour détruire des informations, espionner la machine victime, offrir une connexion aux machines des adversaires, ou utiliser les ressources de la machine victime pour exécuter d'autres attaques.

- Cheval de Troie (« trojan »). C'est un type de virus où le code malveillant est caché dans un programme bénin. Son but, plutôt que de se propager dans le réseau, est de permettre aux adversaires d'exécuter d'autres logiciels malveillants dans les machines victimes.

- Porte dérobée (« backdoor »). C'est un logiciel malveillant qui permet aux adversaires de contourner le processus d'authentification et de contrôle d'accès pour prendre le contrôle des machines victimes. Généralement, elles sont installées dans les machines victimes par les chevaux de Troie. Après, les adversaires les utilisent pour accéder à la machine victime à l'insu des usagers.

- Bombe logique. C'est une partie d'un vers ou cheval de Troie qui a été programmée pour s'activer à l'occurrence de certaines conditions. Les conditions peuvent être une date particulière, une valeur particulière d'un paramètre, un usager particulier qui accède au système, etc. Une fois que la bombe logique est activée, elle exécute un code malveillant avec un but spécifique, généralement visant à altérer le fonctionnement normal du système.
- Vulnérabilité « zero-day ». Ce terme fait référence aux défaillances logicielles ou matérielles qui restent inconnues jusqu'au lancement d'un ver informatique qui les exploite. Cela signifie que les vulnérabilités sont inconnues pour les développeurs de logiciels, les fabricants de matériels et les développeurs des logiciels antivirus, mais elles ne sont pas inconnues pour les adversaires. Donc, les adversaires profitent du fait qu'il n'existe aucun correctif pour ce type de vulnérabilité et se servent d'elles pour exécuter de nouvelles attaques.

En plus des logiciels malveillants, les systèmes de contrôle industriels sont aussi susceptibles d'être la proie de pirates informatiques professionnels, aussi connus sous le nom de menace persistante avancée (« Advanced Persistent Threat »). Cette terminologie fait référence aux attaques très sophistiquées contre des systèmes ciblés où les adversaires sont des groupes d'individus hautement qualifiés, supportés par des groupes terroristes ou des gouvernements. Elles sont exécutées aux fines d'espionner ou de saboter le système ciblé, soit par des motivations économiques ou politiques. Ces attaques se caractérisent par : 1) une longue période d'exploration et reconnaissance du système pendant laquelle l'attaque reste indétectable, 2) l'usage des logiciels malveillants très élaborés et sophistiqués, et 3) une planification et préparation minutieuses [67] [68].

3.4 Les attaques informatiques contre les systèmes de contrôle industriels

Dans les sections précédentes, nous avons présenté les caractéristiques des systèmes de contrôle industriels, les raisons pour lesquelles ces systèmes sont aujourd'hui susceptibles de subir des attaques informatiques, et les attaques et menaces informatiques auxquels ils sont exposés. Dans cette section, nous présentons une sélection de vraies attaques intentionnelles qui ont été lancées contre des systèmes de contrôle et des infrastructures critiques se trouvant dans différentes parties

du monde. Cela démontre que le risque de subir des attaques informatiques est réel et que les techniques utilisées par les attaquants sont de plus en plus sophistiquées.

Au début de l'année 2000, le système de contrôle des eaux usées du Conseil de Maroochy Shire à Queensland, Australie, a subi une attaque informatique qui a occasionnée le déversement d'environ un million de litres d'eaux usées non traitées dans un drain d'eaux pluviales convergeant vers des cours d'eau locaux [69]. Cette attaque a été perpétrée par un ex-employé de l'entreprise qui avait fourni le système de contrôle. Dans un premier temps, l'employé a été licencié par ladite entreprise, puis il a demandé un emploi au Conseil de Maroochy Shire et il a été refusé. Par vengeance, il a décidé d'attaquer le système et de faire passer l'attaque par un mauvais fonctionnement du système. Avant de quitter l'entreprise, l'attaquant aurait installé dans son laptop le programme de configuration du système SCADA, et aurait volé des radios et des dispositifs de contrôle utilisés pour commander les pompes. En se servant de cet équipement et des faiblesses d'authentification du réseau de communication, l'attaquant s'est fait passer par une entité légitime du réseau de contrôle et il a réussi à manipuler les pompes et les valves du système à volonté. Cette attaque a mis en évidence qu'attaquer un système contrôlant des infrastructures critiques peut causer des dommages qui vont bien au-delà de la destruction de fichiers ou de la divulgation d'informations.

En 2010, environ 14 installations industrielles en Iran ont été infectées par le ver Stuxnet [70]. C'est un ver très sophistiqué qui a été conçu pour exploiter des vulnérabilités informatiques des PLC Siemens contrôlant les centrifugeuses de centrales d'enrichissement d'uranium. Stuxnet a utilisé quatre vulnérabilités « zero-day », des techniques avancées pour n'être détecté ni par les usagers ni par les logiciels antivirus, en utilisant des certificats de sécurité légitimes, mais volés, pour signer ses pilotes et s'installer dans les machines infectées [71]. Le ver aurait été introduit dans le système depuis une clé USB des prestataires externes. Une fois dans le système, il a exploité des vulnérabilités « zero-day », a infecté d'autres clés USB, et s'est reproduit et s'est inséré dans les ressources du réseau partagés, afin de se propager pour se rendre à sa destination finale : les PLC. Lorsqu'il est arrivé aux PLC, il les a infectés avec un exploit de vulnérabilité « zero-day » permettant de modifier leur programmation [40]. En raison de la nouvelle programmation, plusieurs centrifugeuses ont été endommagées ou détruites. Jusqu'ici, l'identité des créateurs de Stuxnet n'a pas été confirmée, mais il y a des spéculations que cette attaque a été planifiée et supportée par des gouvernements des pays ennemis de l'Iran. Cette attaque met en avant que des

systèmes peuvent quand même être victimes des attaques informatiques même s'ils ne sont pas connectés à l'Internet.

En 2014, une aciérie en Allemagne a été victime d'une attaque informatique qui a causé des dommages matériels importants [72]. Selon l'information disponible analysée, l'attaquant a utilisé l'hameçonnage et a envoyé des courriels contenant un code malicieux aux opérateurs de l'aciérie. En utilisant le code malicieux, l'attaquant a gagné accès au système des affaires, puis il a accédé au système de contrôle. Après avoir accédé au système de contrôle, il a détruit les éléments des interfaces des opérateurs et il a contourné les mécanismes pour éteindre la chaudière de façon sécuritaire, ce qui a entraîné des dommages physiques massifs. Les indices ont démontré que l'attaquant possédait des connaissances solides du système et, à partir de la magnitude du dommage produit, les experts affirment que l'attaquant ne serait pas un individu, mais un groupe particulier. De plus, l'attaque démontre que bien que les systèmes soient munis de mécanismes de sécurité pour les protéger des attaques informatiques, les attaquants réussissent à trouver un point faible à exploiter. Pour cette occasion, c'étaient les opérateurs.

En décembre 2015, une attaque informatique contre les systèmes SCADA de trois compagnies de distribution d'électricité en Ukraine a causé plusieurs pannes d'électricité qui ont impacté environ 225 000 personnes dans huit provinces de ce pays [73] [74]. L'attaque a commencé longtemps avant décembre 2015. D'abord, les attaquants ont accédé aux réseaux d'entreprise en infectant les ordinateurs du personnel et des administrateurs des systèmes d'affaires avec un logiciel malveillant qui ouvrait une porte dérobée pour les attaquants à l'insu des usagers. Le logiciel malveillant a été implanté dans des fichiers Word et Excel attachés aux courriels d'harponnage qui ont été envoyés aux travailleurs sélectionnés. Dans cette étape, les attaquants ont récolté les identifiants usagers et les mots de passe des opérateurs et ils ont découvert des réseaux virtuels privés utilisés par les opérateurs pour se connecter à distance aux systèmes SCADA. En se servant de ces ressources, les attaquants ont accédé aux réseaux de contrôle. Puis, ils ont fait l'exploration et reconnaissance des réseaux de contrôle afin d'apprendre leur architecture et d'identifier les éléments à utiliser pendant l'attaque. Ensuite, le 25 décembre, les attaquants se sont connectés aux systèmes SCADA à travers les réseaux virtuels privés découverts, ils ont pris le contrôle des ordinateurs des opérateurs et ils ont commandé l'ouverture à distance des interrupteurs dans 30 postes électriques. Mais cette attaque n'a pas été conçue seulement pour interrompre la distribution d'électricité, elle visait aussi

à empêcher que les opérateurs puissent rétablir le service normal le plus rapidement possible. Pour cela, les attaquants ont complémenté l'attaque avec les actions suivantes :

- Reprogrammation du système d'alimentation ininterrompue servant aux centres de contrôle de deux des compagnies attaquées pour qu'il s'arrête une fois l'attaque soit lancée. Cette action a laissé sans électricité les réseaux d'ordinateurs et les opérateurs dans les centres de contrôle de ces compagnies.
- Remplacement du micrologiciel des convertisseurs série-Ethernet de plus de 12 postes électriques par un micrologiciel malicieux qui a rendu les convertisseurs par la suite inutilisables, irrécupérables, et incapables de recevoir des commandes. Cette action a empêché la fermeture à distance des interrupteurs ouverts, donc les opérateurs ont été obligés de se rendre aux postes électriques pour refermer les interrupteurs afin de rétablir le service.
- Utilisation d'une bombe logique pour activer un logiciel malveillant qui a effacé les fichiers contenus dans les ordinateurs des opérateurs, y compris le registre principal de démarrage. Cette action a causé la panne des ordinateurs des opérateurs.
- Attaque de déni de service contre le centre d'appel pour empêcher les clients d'appeler pour signaler la panne. Cette action visait à éviter que les opérateurs soient informés de l'occurrence et du déroulement de l'attaque.

La présence de nombreuses vulnérabilités ainsi que l'existence documentée de plusieurs incidents de cyber sécurité dans les réseaux de contrôle industriels démontre qu'il est nécessaire de considérer la sécurité des réseaux de contrôle, notamment des réseaux de contrôle du trafic routier.

3.5 Évaluation de la menace

Dans cette section, nous présentons un résumé des efforts pour quantifier la menace liée aux cyberattaques dans les réseaux de contrôle. Nous montrons des travaux où la co-simulation a été utilisée pour étudier la sécurité informatique des systèmes cyber-physiques en général. Ensuite, nous présenterons des travaux qui ont évalué la sécurité informatique des systèmes de contrôle de trafic routier spécifiquement. Plus de détails sur les travaux présentés ici sont donnés à la section 5.3 de ce mémoire.

3.5.1 Usage de la co-simulation pour évaluer la sécurité informatique des systèmes cyber-physiques

Huang *et al.* [75] ont utilisé la co-simulation pour évaluer les impacts physiques et économiques d'attaquer un système contrôlant un réacteur nucléaire. Ils ont exécuté des attaques d'intégrité ciblant l'information des capteurs et des actuateurs, des attaques de déni de service ciblant des senseurs et des capteurs, et des attaques visant à produire un impact économique négatif, c'est-à-dire, des attaques menant à l'augmentation des coûts de production. Cette expérimentation a permis d'identifier : 1) le type d'attaque (ou la combinaison d'attaques) produisant le plus d'impact sur le processus physique (comme mener le système à un état dangereux ou augmenter les coûts de production), et 2) les composants les plus critiques du processus de contrôle, c'est-à-dire, ceux qui produiraient le plus d'impact s'ils étaient attaqués. Une telle information sert à établir (ou renfoncer) les mesures de défense, tant afin de favoriser la protection des dispositifs critiques que pour empêcher les attaques les plus nocives.

Krotofil et Larson [76] ont utilisé la co-simulation pour évaluer les effets de cyber attaques contre un système contrôlant une usine chimique. Le scénario est basé sur les modèles des usines chimiques de Tennessee Eastman et du monomère d'acétate de vinyle. Ce scénario peut être utilisé de façon autonome pour exécuter des attaques réseau ou des attaques ciblant tant les actuateurs que la logique de contrôle du système. De plus, en le connectant à un réseau de contrôle, il est possible d'étudier les conséquences que produiraient des attaques contre les éléments de contrôle, comme les PLC, sur le processus physique. Il permet aussi d'évaluer l'effectivité de mécanismes de défense, comme les systèmes de détection d'intrusions, pendant ces attaques.

Bernieri *et al.* [77] ont utilisé le scénario de co-simulation pour le diagnostic de défauts dans les infrastructures critiques (« Fault Diagnosis Approach for Critical Infrastrustures », FACIES) [78] pour évaluer la performance d'un module de diagnostic de défauts (« fault diagnosis module ») durant des attaques informatiques contre un système de distribution d'eau. Ils ont aussi intégré un système de détection d'intrusion au réseau de contrôle pour supporter le module de diagnostic de défauts. Ensuite, ils ont exécuté des attaques de déni de service, de modification de paquets et de rejeu, afin d'évaluer l'efficacité et la fiabilité du schéma de protection.

Lemay, Fernandez et Knight [79] se sont servis de la co-simulation pour évaluer les impacts de cyberattaques contre un système contrôlant un réseau électrique. Le scénario utilise un cluster

virtualisé qui émule un réseau informatique [80] avec un simulateur de flux de puissance électrique. Ils ont reproduit des attaques de déni de service, d'infection par malware, de falsification de données et d'injection de paquets contre le système, et ils ont évalué leurs impacts tant sur le réseau de contrôle que sur le réseau électrique.

3.5.2 Évaluation de la sécurité informatique des systèmes de contrôle du trafic routier

Ernst et Michaels [81] ont présenté un cadre pour évaluer l'impact de vulnérabilités informatiques associées à quatre niveaux d'accès aux contrôleurs de feux de circulation et en considérant la demande de trafic aux carrefours. Les différents niveaux d'accès identifiés comme étant susceptibles aux attaques informatiques étaient : 1) les détecteurs des véhicules, 2) le signal de synchronisation des contrôleurs de feux, 3) l'accès à distance aux contrôleurs de feux, et 4) l'accès physique au cabinet de contrôle. En s'appuyant sur le logiciel de simulation de trafic routier « Simulation of Urban Mobility » (SUMO) [82], ils ont créé un corridor routier coordonné et l'ont utilisé pour évaluer les impacts des attaques associées aux niveaux 1, 2 et 3. L'évaluation de l'impact des attaques associées au niveau 4 a été faite en considérant que l'adversaire a accédé au cabinet du contrôleur et a neutralisé l'opération de l'unité de gestion de conflits. Les résultats ont montré que les attaques aux niveaux 1 et 2 impactent le temps de parcours tandis que les attaques aux niveaux 3 et 4 impactent la sécurité des usagers. Particulièrement, ces dernières attaques permettent d'altérer les paramètres des plans de feu sans respecter les contraintes de sécurité et de contourner l'actuation de l'unité de gestion de conflits pour mettre l'ensemble de feux dans une condition dangereuse, comme le feu vert dans toutes les approches. Enfin, ce travail s'est appuyé seulement sur la simulation pour évaluer l'impact de diverses attaques informatiques contre les contrôleurs de feux de circulation d'un corridor synchronisé.

Ezell, Robinson, Foytik, Jordan et Flanagan [83] ont estimé l'impact économique d'une attaque informatique contre un système de contrôle de tunnels routiers. Puisque le système est isolé, ils ont modelé une attaque type Stuxnet où un code malveillant aurait été inséré dans le système de contrôle depuis la clé USB de l'un des opérateurs. Une fois inséré, le code resterait inaperçu dans le système jusqu'à ce que les capteurs détectent une forte pluie. À ce moment-là, il éteindrait et allumerait cycliquement les ventilateurs et les pompes à l'intérieur du tunnel provocant une situation dangereuse, menant à la fermeture du tunnel. En s'appuyant sur la simulation, les auteurs

ont reproduit les conditions du trafic dans la région d'étude pendant les heures de pointe du matin et ils ont estimé l'impact économique que produirait la fermeture du tunnel pendant cette période de la journée. L'impact économique estimé a été calculé en multipliant l'augmentation du temps de parcours global dans la région (calculé à partir des résultats de la simulation) par le coût moyen courant d'une heure de travail. Cette approche utilise la simulation pour reproduire les conditions du trafic pendant une attaque informatique et obtenir les métriques nécessaires pour estimer l'impact économique de l'attaque. Cependant, la partie cyber du système de contrôle du trafic n'est pas intégrée à l'expérimentation, ce qui ne permet pas d'exécuter des attaques contre le réseau de contrôle et d'évaluer leurs impacts.

Les travaux présentés dans la section 3.5.1 ont montré l'usage de la co-simulation pour évaluer la sécurité informatique de divers systèmes de contrôle industriels, mais aucun d'entre eux ne montre son utilisation dans le domaine de contrôle du trafic routier. Par contre, les travaux présentés dans cette section, qui ont porté sur l'évaluation de la sécurité des systèmes de contrôle du trafic routier, se sont appuyés seulement sur la simulation sans inclure le composant de contrôle du système, ce qui limite la portée des évaluations.

3.6 Conclusion

Dans ce chapitre, nous avons dressé un portrait de la sécurité informatique des systèmes de contrôle industriels, en incluant les systèmes de contrôle du trafic routier. L'information présentée ici a fait ressortir que : 1) les menaces pesant sur les systèmes contrôlant les infrastructures critiques sont réelles, 2) les facteurs qui attentent le plus contre la sécurité informatique des systèmes de contrôle actuels sont l'interconnexion des réseaux de contrôle avec d'autres systèmes ou réseaux et la disposition d'information sur l'Internet qui peut être utilisée pour les attaquer, et 3) les techniques utilisées pour les attaquants sont de plus en plus sophistiquées. En ce qui concerne les systèmes de contrôle du trafic routier, nous avons présenté des indices qui démontrent qu'ils sont aussi susceptibles à subir des attaques informatiques à cause tant des vulnérabilités informatiques existantes dans leurs composants que du manque de politiques de sécurité adéquates.

Finalement, nous avons présenté une sélection de travaux antérieurs qui ont porté sur la sécurité informatique des systèmes de contrôle industriels. Cette littérature a fait ressortir que l'intégration tant du composant de contrôle que du processus contrôlé dans un même scénario d'expérimentation

(co-simulation) permet d'évaluer comment des attaques lancées contre les composants de contrôle impactent le processus physique. Cependant, jusqu'ici, les travaux portant sur l'évaluation de la sécurité des systèmes de contrôle du trafic routier ont utilisé la simulation pour évaluer le comportement de la circulation routière face à certaines attaques, mais ils n'ont pas intégré le composant de contrôle du système. C'est dans cette optique que nous avons développé un banc d'essai basé sur la co-simulation pour évaluer comment des attaques informatiques lancées contre les éléments qui contrôlent le trafic routier impactent la circulation dans les réseaux routiers. Le banc d'essai est décrit dans l'article « A cyber-physical test bed to measure the impacts of cyber attacks in urban road networks », qui a été présenté à la « Twelfth IFIP WG 11.10 International Conference on Critical Infrastructure Protection », en mars 2018, est qui se montre au chapitre 5 de ce mémoire.

Dans le prochain chapitre, nous montrerons comment la démarche présentée dans ledit article nous a permis d'atteindre deux des objectifs spécifiques proposés au début de notre recherche. Ultérieurement, dans le chapitre 6 nous montrerons la démarche complémentaire que nous avons empruntée pour atteindre le reste des objectifs.

CHAPITRE 4 DÉMARCHE DU TRAVAIL DE RECHERCHE

À la section 1.3 de ce mémoire, nous avons énoncé que l'objectif principal de notre recherche était de mesurer l'impact des attaques informatiques sur le réseau de contrôle du trafic routier. Pour atteindre cet objectif, nous avons divisé la démarche de notre recherche en quatre étapes, chacune d'elles visant à accomplir un des objectifs spécifiques suivants :

1. Développer un banc d'essai pour reproduire les systèmes contrôlant le trafic dans des réseaux routiers.
2. Reproduire expérimentalement des attaques informatiques sur les contrôleurs de feux de circulation d'un réseau routier.
3. Reproduire expérimentalement l'état de la circulation dans un réseau routier de Montréal en conditions normales et pendant une attaque informatique sur les feux de circulation.
4. Mesurer les coûts économiques des attaques, en fonction du retard global résultant de l'attaque sur le réseau.

Dans ce chapitre, nous ferons le lien entre les objectifs de cette recherche avec l'article de conférence présenté au chapitre suivant.

4.1 Démarche

Dans le chapitre antérieur, nous avons montré qu'une partie des travaux réalisés, associés à la sécurité des systèmes de contrôle du trafic routier, visaient à démontrer que des éléments des systèmes actuels possèdent des vulnérabilités informatiques qui peuvent être exploitées par des individus malveillants. En effet, Ghena *et al.* [13] et Cerrudo [14] ont réussi à manipuler des feux de circulation dans certaines villes aux États-Unis en exploitant des vulnérabilités détectées dans les systèmes déployés. D'autres travaux visaient à évaluer les impacts sur le trafic routier des attaques informatiques contre les éléments de contrôle. Dans ces cas, les auteurs se sont servis de la simulation pour reproduire le comportement du trafic pendant les attaques. Aussi, on a présenté des travaux où les bancs d'essai (« testbed ») basés sur la co-simulation ont été utilisés pour étudier la sécurité informatique de divers systèmes de contrôle industriels. Ces travaux ont mis en évidence que les approches basées sur la co-simulation permettent d'évaluer comment des attaques

informatiques contre le système de contrôle et ses composants impactent le processus physique contrôlé. Cela démontre que l'intégration du composant de contrôle avec le processus contrôlé dans un banc d'essai, produit l'option la plus appropriée pour étudier avec une grande fidélité et à faible coût les effets des attaques informatiques contre les systèmes contrôlant des processus physiques. Cependant, à ce jour, aucun des travaux répertoriés dans la littérature ne montre l'usage de la co-simulation pour reproduire des attaques informatiques contre les systèmes de contrôle du trafic routier et mesurer leurs impacts sur le trafic. C'est pour cela que nous avons dû développer un banc d'essai basé sur la co-simulation nous permettant d'atteindre l'objectif principal de notre travail de recherche : mesurer l'impact des attaques informatiques sur le réseau de contrôle du trafic routier.

Le banc d'essai développé est détaillé dans l'article « A cyber-physical test bed to measure the impacts of cyber attacks in urban road networks », au chapitre 5 de ce mémoire. Cet article a été présenté à la « Twelfth IFIP WG 11.10 International Conference on Critical Infrastructure Protection », en mars 2018.

Voici le contenu de l'article est sa relation avec les objectifs de cette recherche :

La section 5.1 présente l'introduction du travail. Elle montre de façon résumée la problématique abordée dans cette recherche et les objectifs envisagés.

La section 5.2 présente des notions élémentaires du contrôle de trafic routier. La plupart de l'information montrée dans cette section est incluse dans le chapitre 2 de ce mémoire.

La section 5.3 contient une sélection de travaux antérieurs liés à la sécurité informatique des systèmes de contrôle industriels et des systèmes de contrôle du trafic routier. Cette section reprend donc des éléments des travaux montrés à la section 3.5 de ce mémoire.

La section 5.4 montre les exigences fonctionnelles du banc d'essai. Ce sont les aspects techniques que doit réunir le banc d'essai afin qu'il soit capable de : 1) reproduire un système contrôlant le trafic dans les réseaux routiers, 2) reproduire de différentes attaques informatiques contre les éléments du système de contrôle du trafic routier, et 3) mesurer l'impact des attaques.

La section 5.5 montre l'architecture du banc d'essai et décrit les caractéristiques de ses composants. Le banc d'essai contient une partie cyber, constituée par les éléments qui contrôlent le trafic routier, et une partie physique, constituée par le trafic dans les réseaux routiers. La partie cyber est intégrée par l'application ScadaBR, qui émule les fonctions de surveillance et contrôle centralisés d'un

système SCADA, et des scripts python qui reproduisent les fonctions des PLC qui contrôlent les feux de circulation dans le réseau routier. Pour reproduire les réseaux et le trafic routiers (partie physique), nous avons choisi SUMO (« Simulation of Urban Mobility ») qui est une application de simulation microscopique du trafic routier. Ces deux parties communiquent entre elles à travers d'un serveur TCP développé en python. Avec le développement du banc d'essai décrit, nous avons atteint le premier des objectifs énonces : développer un scénario expérimental pour reproduire un système contrôlant le trafic dans des réseaux routiers.

La section 5.6 décrit le scénario d'expérimentation que nous avons utilisé pour valider l'intégration et la fonctionnalité du banc d'essai. Dans un premier temps, nous avons exécuté différentes attaques informatiques contre les contrôleurs des feux de circulation. Ensuite, nous avons reproduit un petit réseau routier intégré par trois carrefours à feux isolés et nous avons attaqué l'un des feux de circulation de ce réseau pour évaluer l'impact des attaques. Ultérieurement, nous avons reproduit le corridor routier coordonné qui a été utilisé par Ernst et Michaels [84] et nous avons attaqué l'un des feux de circulation du corridor. À partir de ces expérimentations nous avons vérifié que le banc d'essai est capable de reproduire différentes attaques informatiques contre les contrôleurs des feux de circulation et aussi de reproduire divers scénarios d'attaque sur les réseaux routiers. Cette section nous a permis d'accomplir le deuxième des objectifs établis : reproduire expérimentalement des attaques informatiques sur les contrôleurs de feux de circulation d'un réseau routier.

La section 5.7 montre les résultats des tests exécutés à la section précédente. Ces résultats démontrent que les attaques exécutées ont impacté le temps de parcours et la longueur des files d'attente, non seulement pour les voitures se trouvant sur les approches des carrefours attaqués, mais aussi pour les voitures se trouvant sur les autres tronçons des réseaux modélisés. Cette section a mis en évidence que les impacts des attaques informatiques contre les réseaux routiers peuvent être mesurés à partir des métriques fournies par SUMO. Cela nous approche de l'objectif principal de notre recherche : mesurer l'impact des attaques informatiques sur le réseau de contrôle du trafic routier.

La section 5.8 présente les conclusions et les limitations de la démarche montrée dans l'article. Cette section fait ressortir que l'usage de la co-simulation dans le banc d'essai favorise l'étude des résultats émergents, comme le fait qu'attaquer l'un des feux de circulation du corridor impacte la circulation dans tous les tronçons du corridor, et que ce type de résultats ne pourrait pas être détecté

avec l'usage de bancs d'essai basés seulement sur la simulation. D'autre part, cette section suggère d'utiliser le banc d'essai pour évaluer les impacts d'attaques informatiques sur des modèles de réseaux routiers plus représentatifs des réseaux routiers réels.

4.2 Conclusion

La démarche présentée dans l'article nous a permis d'atteindre deux des objectifs spécifiques énoncés au début de la recherche : développer un scénario expérimental pour reproduire un système contrôlant le trafic dans des réseaux routiers, et reproduire expérimentalement des attaques informatiques sur les contrôleurs de feux de circulation d'un réseau routier.

Aussi, elle a montré que le banc d'essai proposé permet de mesurer l'impact des attaques informatiques contre le réseau de contrôle du trafic routier à partir des métriques, telles que le temps de parcours ou la longueur de la file d'attente, fournies par la simulation du trafic routier. Cependant, dû à la simplicité du modèle utilisé pour la validation, deux des objectifs spécifiques énoncés ne sont pas atteints. Ceux-ci sont : reproduire expérimentalement l'état de la circulation dans un réseau routier de Montréal (en conditions normales et pendant une attaque informatique sur les feux de circulation) et mesurer les coûts économiques des attaques, en fonction du retard global résultant de l'attaque sur le réseau. C'est dans cette optique qu'une expérience complémentaire a été réalisée à partir d'un modèle du réseau routier plus représentatif. Cette démarche complémentaire est décrite au chapitre 6 de ce mémoire.

CHAPITRE 5 ARTICLE 1 : A CYBER-PHYSICAL TEST BED FOR MEASURING THE IMPACTS OF CYBER ATTACKS ON URBAN ROAD NETWORKS

Authors: Marielba Urdaneta, Antoine Lemay, Nicolas Saunier, Jose M. Fernandez

École Polytechnique de Montréal, Montréal, Canada

marielba-margarita.urdaneta-velasquez@polymtl.ca, antoine.lemay@polymtl.ca, nicolas.saunier@polymtl.ca, jose.fernandez@polymtl.ca

Presented at the Twelfth IFIP WG 11.10 International Conference on Critical Infrastructure Protection, March 2018

Abstract: Efficient and safe transportation of people and goods is a key requirement for the economy to prosper. Traffic control systems are installed at complex intersections to ensure the safe and efficient flow of traffic. However, what if an adversary were to take advantage of the existing security flaws in traffic control systems to create a cyber attack? In this paper, we present a co-simulation framework for cyber-physical systems that allows researchers to reproduce computer-based attacks targeting traffic control systems and measure the impact of those attacks on road traffic. This solution integrates an emulated Supervisory Control and Data Acquisition (SCADA) system with a microscopic traffic simulation tool to provide the functions of a traffic signal control system. The impact of the cyber attacks on road traffic can be measured from the outputs provided by the traffic simulation. Experimental results for a corridor of six coordinated signalized intersections are presented, where the impact is measured in terms of vehicle travel time and queue length. The physical impacts of compromising a single intersection could be felt at other intersections in the road network. This type of emergent result could only have been observed in such a co-simulation framework.

Keywords: Computer security; cyber-physical systems; road traffic control; control process networks.

5.1 Introduction

Traffic congestion is a growing problem and road safety remains an issue in many cities around the world [5]. Traffic congestion not only impacts the economy and the environment of cities, but also the quality of life and health of their inhabitants. To mitigate congestion, cities are constantly looking for measures to improve and expand their traffic infrastructure and public transportation systems. Traffic infrastructure not only comprises road networks, but also traffic control devices, such as signs, markings and traffic signals, which regulate and control traffic at intersections. Traffic signals and sensors can be connected to centralized systems responsible for collecting real-time traffic data, analyzing this data and implementing subsequent control strategies. These control strategies seek to optimize traffic conditions, increase network capacity and user safety. Moreover, they intend to reduce delays, stops, fuel consumption and pollutant emissions originating from traffic lights operations.

Current traffic signal control systems are typically integrated using traffic light controllers, sensors, communication networks and a computer-based central system controlling traffic signals and monitoring traffic conditions and equipment status [7]. However, as newer technology is introduced, the system is exposed to more cyber risks. For example, recent trends show that wireless technology is being increasingly used in both communication networks and traffic detection, due to its low maintenance costs and high scalability potential [18] [19].

Despite its benefits, wireless technology introduces some security risks that make traffic signal control systems vulnerable to cyber attacks. In particular, wireless communication networks are remotely accessible. Once the communication network is accessed, the control network is exposed and vulnerable to be hacked, as demonstrated by Cerrudo [14] and Ghena *et al.* [13]. They detected vulnerabilities related to the lack of authentication (or poor authentication mechanisms) while accessing both wireless network components and traffic light controllers, and the lack of communication encryption. Due to these conditions, the researchers could control traffic signals by capturing and modifying wireless communication, sending fake data and commands to traffic light controllers, and connecting to controllers in order to alter their programming.

Imagine that an adversary takes advantage of existing security flaws in traffic control systems to create a cyber attack. How would the attack impact road congestion? What would be the economic, environmental and social consequences of such an attack? By having an experimental environment

that faithfully reproduces computer-based attacks on traffic control systems and its effects on road traffic, municipal authorities could measure the impact of this kind of attack in a controlled and safe way prior to the occurrence of real attacks. As a result, they could effectively plan defense strategies to improve security in both communication and process networks and establish adequate measures to mitigate the physical impact of the attacks. Furthermore, it would help authorities determine and implement the best mitigation strategies, according to the impact of the attacks, thus facilitating adequate decision making during actual occurrences of these attacks.

To enable this capability, we developed a co-simulation framework that allows researchers to experimentally reproduce cyber attacks targeting traffic signal control systems, and to evaluate how they impact road traffic in cities. Our approach integrates a microscopic traffic simulation tool and an emulated Supervisory Control and Data Acquisition (SCADA) system to provide the functionalities of a traffic control system. The main purpose of this work is to offer an experimental mechanism to conduct computer security tests in the application domain of road traffic control and that allows quantification of the environmental, economic and social impact of the attacks. It is, to the best of our knowledge, the first cyber-physical test bed based on a co-simulation framework created to conduct computer security research in the road traffic control domain.

This article is organized as follows. We start by reviewing the background on traffic control. Next, in Section 5.3 we present previous research related to computer security of both process control and traffic control systems as well as the usage of co-simulation-based frameworks to assess the impacts of cyber attacks in control process systems. The functional requirements and the architecture of the proposed test bed are explained in Sections 5.4 and 5.5 respectively. Section 5.6 describes the validation setup we developed and the experimental setup we used to execute the attacks. The experimental results are shown in Section 5.7. Finally, we present our conclusions and some insights for future work in Section 5.8.

5.2 Background on traffic control

This section provides some key notions of traffic control, collected from Advance traffic management systems in the Ontario traffic manual [7], Traffic control systems handbook [23], Traffic signal timing manual 2008 [25] and Traffic signals 101 [16].

Traffic is composed of pedestrians, cyclists, vehicles, trucks and on-road public transport that share public roads concurrently. They form traffic movements (or traffic flows) when they move together in the same way and direction. At intersections, two or more traffic movements are considered in conflict if their trajectories cross each other at the same level. In that case, it is necessary to establish which traffic flow has priority over the other (in yield or stop controlled intersections) or when each movement is allowed in the intersection. This assignment is called priority or right-of-way.

Traffic signals are equipped with controllers, which are responsible for switching the lights that indicate to road users when they have the right to move. Controllers may also be connected to vehicle-presence and pedestrian-presence detectors for real time adaptation to traffic demand, and to a Traffic Management Centre (TMC) that monitors and controls road traffic conditions and equipment status in the intersection.

Traffic signal controllers follow a set of rules that establishes the order in which the right-of-way is assigned to the different traffic movements. In addition, the rules establish the green light time duration for each movement. The element that contains all those rules is called the timing plan, whose design and use constitutes the technique most commonly used by traffic engineers to regulate traffic. Timing plans contain control parameters, such as cycle length, phases, splits and intervals. A cycle is a complete sequence of phases, in which the right-of-way has been given to all movements, and the time required to complete that sequence is the cycle length. A phase represents the part of the cycle assigned to a traffic movement, or to several non-conflictual traffic movements simultaneously. The part of the cycle assigned to each phase is the split, and the portion of the cycle during which the lights do not change is an interval. An attacker that would have the capability to alter the configuration of the controllers, i.e. the timing plan, could significantly hamper the flow of traffic.

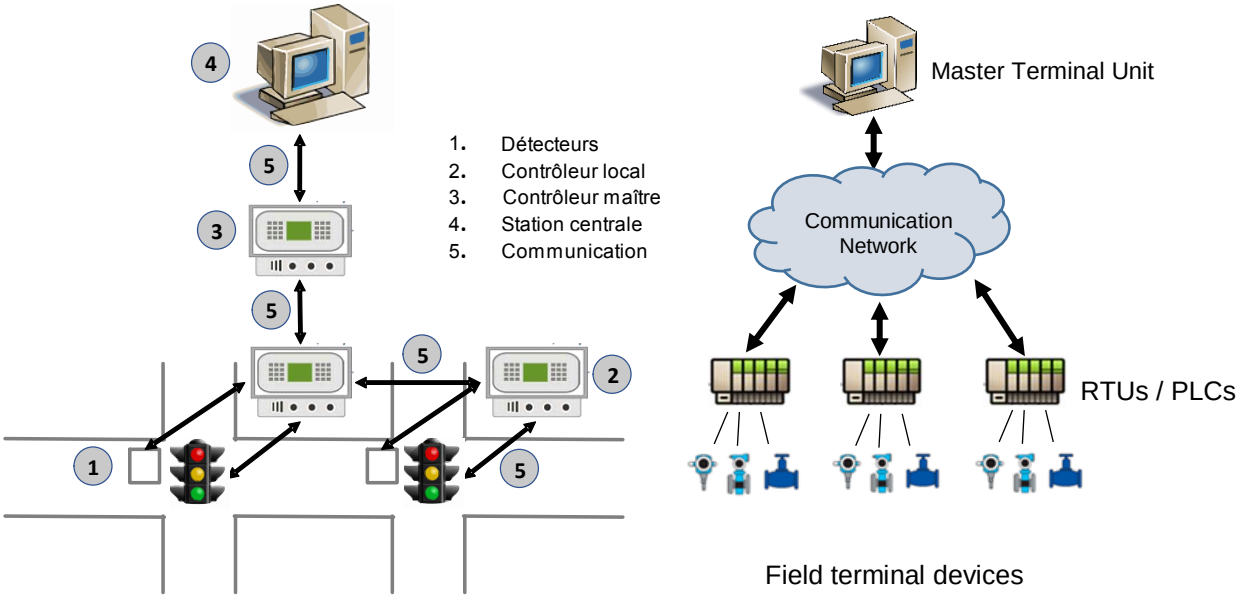
Traffic signals can operate either as isolated nodes or as part of a coordinated system. While working in coordination with other signalized intersections, the time (or offset) between the beginning of the cycles of each successive signalized intersection is computed so that vehicles do not stop at intermediary intersections. Isolated traffic signals are not coordinated and do not consider how neighboring intersections are configured.

Traffic regulation at isolated intersections can be done using pre-timed control, actuated control or a combination of both. Pre-timed traffic lights use pre-elaborated timing plans in which the number,

sequence and duration of phases are fixed. Pre-elaborated plans are calculated using historic traffic conditions at intersections. Actuated traffic lights use traffic condition information, collected by sensors, to activate phases if the presence of vehicles or pedestrians is detected.

Figure 5.1a shows the typical hardware components and architecture of a traffic signal control system. It comprises detectors, local controllers, on-street master controllers, a TMC and communication networks. Detectors are used to determine vehicle presence or pulse duration, needed to calculate vehicle volume, occupancy, speed, etc. Local controllers are responsible for switching head lights at intersections using stored timing plans and schedules previously provided by operators. They receive traffic data from detectors, pre-process it into volume and occupancy parameters, and send it to on-street master controllers. Master controllers are located at intersections and are connected to all local controllers belonging to the same control area to facilitate communication between them and the TMC. They are responsible for selecting traffic responsive timing plans, processing and storing the data collected by the detectors, and monitoring the equipment status at intersections. They communicate with the TMC in the case of critical alarms, on a regular predetermined basis, or when requested by operators. The main function of the TMC is to gather and display information about traffic conditions and intersections equipment status. In addition, it calculates timing plans and the schedules for their selection. Once the timing plans and the selection schedules are generated, they can be downloaded to the on-street master controllers. Furthermore, operators at the TMC can issue commands to master controllers, for example to set the time, or upload information saved in the master controllers.

The above described system has the same distributed architecture, control and monitoring elements as a SCADA network. Basically, a SCADA network controlling an industrial process (depicted in Figure 5.1b) comprises a central station, or Master Terminal Unit (MTU) at the highest control level. It processes the data collected from the field devices, saves it and displays it in the Human-Machine-Interface (HMI) such that the operators can monitor and control the process. MTU are connected to Remote Terminal Units (RTU) or Programmable Logic Controller (PLC). Both RTU and PLC are data acquisition and control devices that are connected to the measurement and control points in the field. They collect the measurement data, convert it and send it to the MTU. Additionally, they process the commands sent from the MTU to the field devices. Finally, the communication network provides the connectivity and the data exchange in the network.



(a) (b)

Figure 5.1: (a) Elements of a traffic signal control system (adapted from [25]) and (b) SCADA network components and architecture

5.3 Related work

5.3.1 Computer security vulnerabilities of process control and traffic control systems

To demonstrate how vulnerable control systems are to cyber attacks, Luallen asked a group of cyber security students to study a process control system governing a physical process in order to find its known vulnerabilities and exploit them [58]. To accomplish this task, students used the Internet to search for information related to the computer security flaws of the chosen system. Next, they hacked it using a commercial cybersecurity training kit. This work demonstrated that nowadays attackers do not require vast knowledge in computer security or any specific skill set to conduct successful attacks against such cyber-physical systems, but also shows that they can readily find on the Internet most of the information they need about their targets. As Luallen's students did, anyone can use Open Source Intelligence (OSINT) tools, and consult existing ICS-

CERT[3] reports, vendor websites and control systems user forums to gather enough information about the target system. Valuable information, such as the system components and architecture, the communication protocols it uses and possible exploits, can be found in this way. Moreover, there are commercial products that can be used to exploit vulnerabilities in the different existing systems.

In the field of computer security of traffic control systems, Cerrudo [14] and Ghena *et al.* [13] detected several security flaws in currently deployed systems in the United States. Even though they studied different systems, they got similar findings which are 1) lack of authentication or poor authentication mechanisms to access traffic light controllers, 2) lack of data encryption, 3) usage of default credentials supplied by the vendors to access traffic light controllers and communication network devices, such as switches, access points or repeaters, and 4) some of the authentication credentials were published in the vendor's website and were not modifiable. In both cases, Cerrudo and Ghena's team could successfully gain access to some of the system components and alter the traffic light state on command.

In their talk, Hack Like a Movie Star [85], Krotofil and A. explained that a successful attack to a cyber-physical system requires the execution of five fundamental steps: 1) gain access to the system, 2) discover the system, 3) take control of the system, 4) cause damage or disruption in the physical process, and 5) clean-up all the evidences pointing to a cyber attack.

To illustrate how this works, they created an experimental cyber-physical test bed that reproduced a system controlling traffic lights in a four-way intersection. They got a commercial control system and a cybersecurity training kit, and used them to assemble the test bed. They could easily obtain access to the system, using the credentials provided by the vendor. Once the system was accessed, they could learn the system configuration and the system behavior by analyzing the information found in the different system tools available on the machine for diagnosis, development and visualization. Additionally, they applied reverse engineering to some captured binary files and communication messages to deduce the link between the information in the monitoring system and its corresponding elements in the physical process. Then, they successfully manipulated traffic

[3] The ICS-CERT is a Computer Emergency Response Team (CERT) created by the US Department of Homeland Security (DHS) specifically to address cyber security issues in Industrial Control Systems.

lights state and operation. Finally, for the attack to remain undetectable, they manipulated the system data so that the operator could not notice the changes in traffic conditions during the attacks. Even though they succeeded in hacking the system, authors emphasized that an attacker must have enough knowledge about how the targeted physical system works to identify the attack that better fulfils the attacker's objectives.

These previous works aimed at demonstrating that existing security flaws in currently deployed traffic signal systems could be exploited by adversaries for successfully hacking traffic signals. However, none of those works measured the impacts of the attacks on traffic congestion or traffic safety.

5.3.2 Usage of experimental scenarios to assess security risks in cyber-physical systems

Experimental setups based on co-simulation frameworks have been used to assess computer security in different cyber-physical systems. In the work of Huang *et al*. [75], it was used to evaluate the impact of computer-based attacks in a process control system governing a chemical reactor. The main objective of this work was to measure the impact of the attacks in the physical process being controlled. Thus, while conducting different types of attacks, the system reaction was modelled and monitored so that the researchers could determine the attack vectors that impacted the physical process the most. They found that, in the steady-state condition of the system, attacks like denial-of-service (DoS) had minor impact on the physical process whereas the combination of DoS attacks with integrity attacks could lead to important damages to the physical system. Furthermore, the authors determined that the operating costs of the system varied depending on the controllers and sensors targeted during the attacks. Krotofil and Larsen [76] developed an open-source framework to control a chemical plant, based on two realistic models: the Tennessee Eastmann (TE) and the Vinyl Acetate Monomer (VAC) chemical plant models. They redesigned prior Matlab models to produce Simulink models of both plants. First, they used the framework alone to conduct cyber attacks targeting sensors and actuators in the physical process. Then, they coupled it to an industrial control network and conducted cyber attacks aimed to capture and modify the data exchanged between the cyber system and the physical system. Another co-simulation framework was used in [77] to evaluate the impacts of cyber attacks on the monitoring elements of a control process system governing a water supply system. This time, Bernieri *et al*.

used the online Fault detection Approach for Critical Infrastructures (FACIES) [78], which is based on a fault diagnosis and intrusion detection architecture, and conducted integrity and availability attacks to evaluate the performance of the fault diagnosis system in effectively detecting them. The tests demonstrated that the fault diagnosis system performed well in detecting replay attacks and attacks targeting actuators state. However, it performed poorly in identifying flooding attacks and attacks targeting sensor information. Results also pointed out that a mediocre performance of the fault diagnosis system, in detecting and identifying the attacks, could induce operators to make unnecessary or erroneous decisions, which could have negative impacts on the physical process. Finally, Lemay, Fernandez and Knight [79] used co-simulation to develop a test bed to evaluate the effects of attacks in both cyber and physical components of an Industrial Control System (ICS) network governing an electric power grid. They used the proven virtualized cluster approach that emulates an IT network with high fidelity described by Calvet *et al.* in [80], and interfaced it with an electrical power flow simulator to reproduce an ICS network controlling an electrical grid. This test bed has proven to be suitable to reproduce network attacks, such as DoS, data falsification (or injection) and malware infection. Moreover, it was efficient to evaluate the impact of the attacks in both the control network and the power grid.

As we can see, test beds based on co-simulation frameworks have been widely used to conduct experimentation in computer security of cyber-physical systems in different domains. However, to the best of our knowledge, none has been built to assess computer security in road traffic control systems.

5.3.3 Threat assessment of traffic control system components

A different approach was adopted by Ernst and Michaels in [84]. They presented a threat assessment framework to evaluate the impact of cyber vulnerabilities providing access to field elements of a traffic control system. More specifically, they distinguished the following four access levels whose security flaws can be exploited by an attacker: 1) vehicle detector, 2) corridor synchronization, 3) traditional Internet, and 4) physical access.

They used the Simulation of Urban Mobility package (SUMO) [82] to simulate a road network consisting of a corridor with six signalized intersection which were either coordinated or isolated, depending on the attack type. Then, they conducted simulated tests to reproduce attacks at access

levels 1, 2 and 3. Accordingly, they measured possible effects of the tests considering different scenarios of traffic demand.

In this case, the traffic simulation was used to reproduce cyber attacks targeting traffic control system elements, and measure the impacts of those attacks on road congestion. However, this simulation-only approach does not include the cyber component of the traffic signals control system. As such, the simulation must rely on broad assumptions of the impact of cyber attacks, and cannot be used to test network defenses. Il faut identifier chaque tableau par un titre. Ce titre, situé au-dessus du tableau est précédé du mot Tableau et d'un numéro d'identification double en chiffres arabes. Il n'y a pas de légende après le titre d'un tableau, c'est dans le texte qu'il faut fournir les explications appropriées. On doit là encore respecter les marges. Si un tableau occupe plus d'une page, il faut en répéter l'identification (tableau, numéro, titre) et ajouter le mot « suite » entre parenthèses. Toutefois, pour éviter d'insérer de longs tableaux dans le texte, il est recommandé de placer en annexe tout tableau trop volumineux.

5.4 Functional requirements of the test bed

Our goal is to design an experimental setup that allows computer security researchers to reproduce cyber attacks targeting traffic control systems and evaluate the impact of those attacks on road traffic in real time. For that, we decided to develop a cyber-physical scenario based on a co-simulation framework to reproduce a two-level distributed control system controlling an urban road network.

One way to accomplish that goal is coupling a monitoring and control system (e.g. a SCADA system) with a microscopic road traffic simulation. On the one hand, the SCADA system provides the required functions to monitor and control in real time large-scale physical processes, such as road networks. On the other hand, traffic simulation is commonly used to reproduce road networks and traffic conditions to plan road traffic control strategies. Additionally, microscopic traffic simulation provides the required information about the different existing entities in road networks, such as pedestrians, vehicles, public transport and traffic lights at a suitable level of granularity.

Moreover, traffic simulation must provide the adequate outputs to measure the economic, environmental and social effects of road congestion resulting from cyber attacking road networks. Some examples of outputs that can be used to measure the impacts are: fuel consumption,

greenhouse gases emissions, pollutant emissions, noise emissions, vehicle density, vehicle travel time, and vehicle waiting time. All that information can be provided by the microscopic traffic simulation.

Finally, it is necessary to incorporate a mechanism to properly couple both the cyber and the physical components of the system. This mechanism will allow us to handle the time difference between the supervisory and control system sampling time, and the traffic simulation step time (if any). Additionally, it will permit the data exchange between the control system and the road traffic simulation.

5.5 Test bed architecture

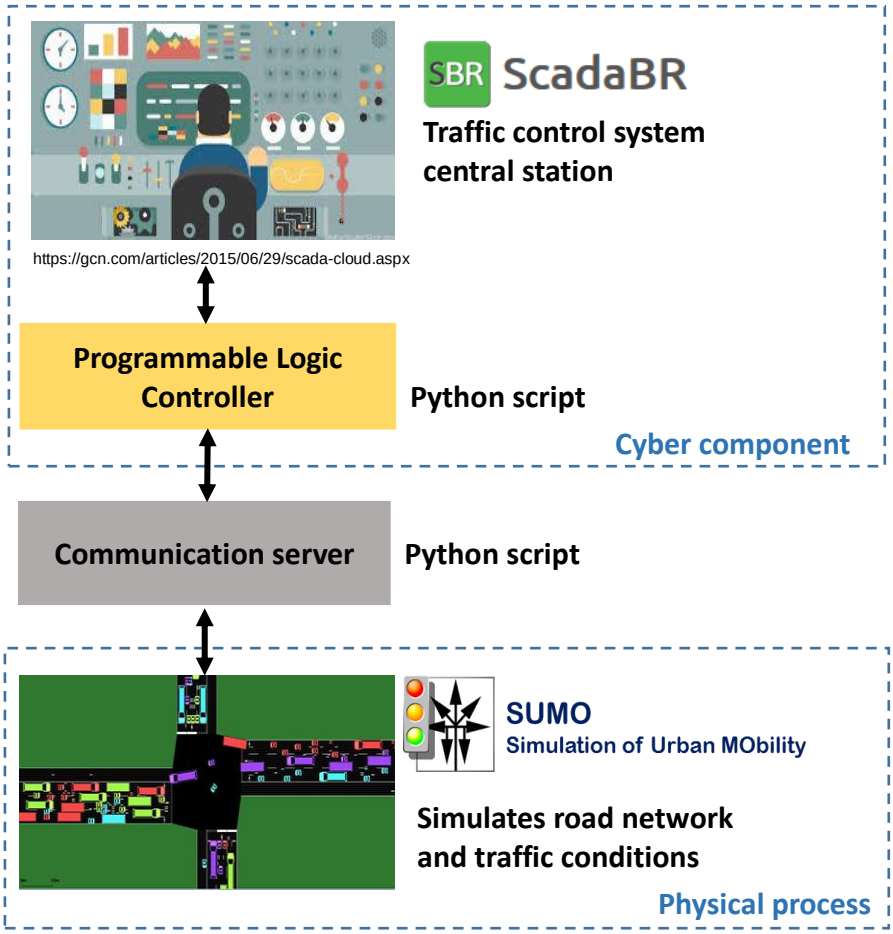


Figure 5.2: General architecture and components of the proposed test bed

With the aim to support the computer security research community with an available, reusable and adaptable platform to test new ideas, we combined different open source software applications to

construct our test bed. Figure 5.2 illustrates this architecture. We describe its details in the following sections.

5.5.1 Monitoring and control system

The high-level control component of the system has been reproduced by using the open source SCADA software ScadaBR 1.0 CE [86]. It is a browser-based SCADA system that 1) provides the monitoring and control functions of a MTU, 2) displays and saves the information about traffic conditions and traffic light states received from the low-level control, 3) enables operators to send commands to change traffic light operation modes (NORMAL/DISABLE), and 4) runs a Modbus client to communicate with each control and data acquisition device in the low-level control. As such, ScadaBR can be configured to accomplish the functions of a TMC to monitor and control several traffic lights.

The low-level control component was implemented using Python scripts that emulate the functions of the PLCs. They read both the MTU commands and the road network data, convert this information and transmit it to the required level. Moreover, they execute the logic to control the traffic signals in the network which means that they act as traffic light controllers. Each PLC is designed to control all traffic signals at one intersection, and it is possible to replicate as many PLCs as there are signalized intersections in the network. Every PLC script runs a Modbus/TCP server to communicate upstream with ScadaBR, using the Modbus/TCP server functionality available in the Modbus TK Python library [87]. In addition, each PLC runs a TCP client to communicate downstream with the road traffic simulation, through a communication server.

5.5.2 Road traffic simulation

In our approach, the physical process to be controlled is the road traffic. To reproduce it, we adopted the open-source microscopic traffic simulation package Simulation of Urban Mobility (SUMO), developed by the German Aerospace Center [82]. SUMO offers the flexibility of creating large-scale road networks from common formats, such as shapefiles or Open Street Map files. Road networks in SUMO include the identification of each signalized intersection and traffic light plans. Additionally, Origin/Destination matrices (OD-matrix) can be converted to single vehicle trips to be loaded in the SUMO simulation.

At each time step SUMO generates outputs giving information about all the simulation elements in the network, such as vehicles, intersections, roads, lanes, traffic lights and inductive loops, among others. This level of granularity is necessary to generate the data that will be measured by the monitoring component. Also, it generates noise emission, pollutant emission and fuel consumption outputs required to quantify the economic, environmental and social effects of road congestion.

SUMO has a Python Traffic Control Interface (TraCI) to interface it with an external application via a TCP socket connection. It permits SUMO to connect to other systems, such as the monitoring and control system. In addition, the TraCI interface allows users to set and modify simulation conditions at any time. For instance, users can change vehicle speeds, driver behavior, road priority or traffic light state as well as force vehicles to change lanes. This is used to enforce state changes dictated by the control component.

SUMO performs a time-discrete simulation, with adjustable step duration from 1 ms and upwards. It also offers two alternatives for the simulation: 1) without visualization, and 2) with visualization through a graphical interface.

5.5.3 Communication server

To properly couple the monitoring and control system with the physical process, we developed a Python TCP multithreaded communication server. Multithreading enables the server to handle and serve multiple concurrent incoming client requests at the same time. Moreover, it allows us to solve any communication synchronization problem related to the difference in time between the PLC sampling interval and SUMO's simulation time step.

At every simulation step, the server receives data and requests from SUMO and the PLCs. On one hand, the data received from SUMO contains the identification of the signalized intersections and the traffic lights states gathered from the simulation. It is stored in a table that matches each signalized intersection with its controlling PLC. Then, the data is sent to the corresponding PLC when requested. On the other hand, the data received from the PLCs contains the identification of the signalized intersection and the traffic light state to be set during the simulation. This data is stored in another table that matches each PLC with its corresponding controlled signalized intersection. Then, it is sent to SUMO when requested.

Using the SUMO TraCI interface, we created a script running a TCP client that at each simulation step transmits the simulation results to the server and requests from it new commands from the PLCs. Then, SUMO adjusts the state of the traffic lights according to the information received from the server.

5.6 Validation and experimental setup

5.6.1 Initial validation

For configuration and testing purposes, we built a preliminary setup in which we connected all the components of our proposed co-simulation framework. Then, we used it to validate: 1) the proper integration of all the components, 2) the proper system operation, and 3) the correct conversion/transmission of the data from the MTU to the traffic simulation, and vice versa.

For the first simulation scenario, the road network contained three signalized intersections, spaced 100 m each and running in pre-timed or semi-actuated mode. To control the traffic lights, we reproduced the control logic described by Krotofil and A. [85], which is based on a finite-state machine that uses eight possible states and nine transition conditions to commute the traffic lights. It also uses four control signals: AUTO, DISABLE, MAIN ROAD and SIDE ROAD. These signals are used to set the traffic lights operation mode from the MTU. When the operation mode is set to AUTO, the traffic lights commute automatically following the finite state machine programming. In this condition, the traffic lights operate in a pre-timed control mode with fixed control parameters. Moreover, timing plans can be changed by modifying the timing conditions and the state sequence in the finite state machine programming. If the operation mode is set to DISABLE, the lights are set to yellow for all directions at the intersection, and will remain in this condition until the DISABLE signal is no longer set. When either the MAIN ROAD or the SIDE ROAD signal is set, the traffic lights operate in a semi-actuated control mode. It means that the green light is assigned to the corresponding road (MAIN or SIDE) until vehicles in the opposite road are detected.

All the system components were installed and configured in a desktop computer running the Windows 10 operating system. SUMO, the TraCI simulation update script and the communication server were running directly in the computer. ScadaBR and the PLCs were running in virtual machines. More specifically, ScadaBR and PLC 1 ran in WindowsXP virtual machines, and PLC

2 and PLC 3 ran in Ubuntu Linux virtual machines. All virtual machines were created using VMWare Workstation software. The interconnection of all these elements is shown in Figure 5.3.

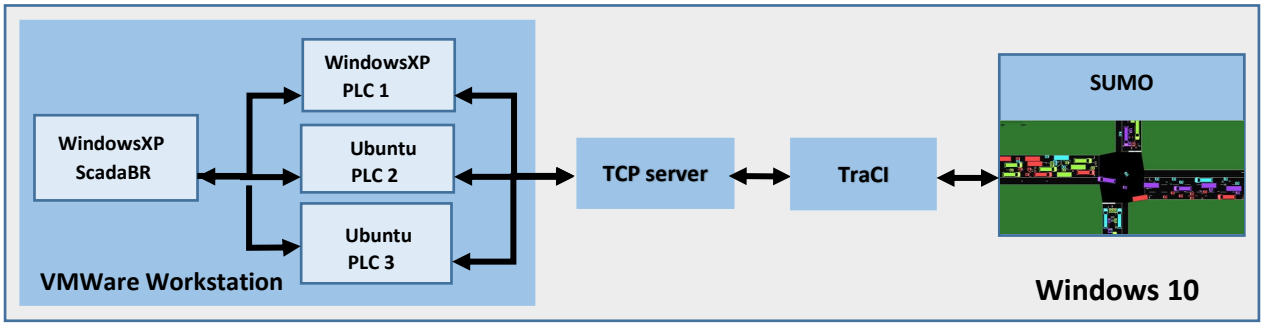


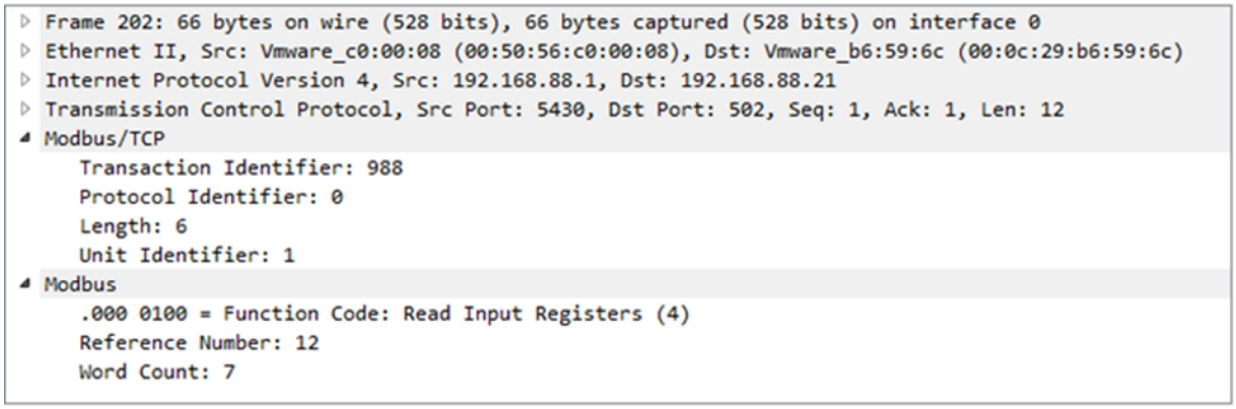
Figure 5.3: System used in the validation

After validating the integration and proper operation of our preliminary setup, we executed computer-based attacks to evaluate the veracity of the proposed test bed. For that purpose, we configured a Kali-Linux virtual machine connected to the same network to which the PLCs and ScadaBR were connected. Using this Kali-Linux machine as the attacker's machine, we conducted man-in-the-middle (MITM) packet capture attacks and packet injection attacks. Our scenario assumed that an attacker had gained access to the communication network, and intercepted the data exchanged between de MTU and the controller. Since the Modbus communication protocol does not use any authentication nor encryption mechanism, attackers can inject control packets on the network that will be accepted by the traffic controller. Furthermore, using information available on the Internet, it is easy to reproduce the content of Modbus messages to generate arbitrary control messages and send them to the controller.

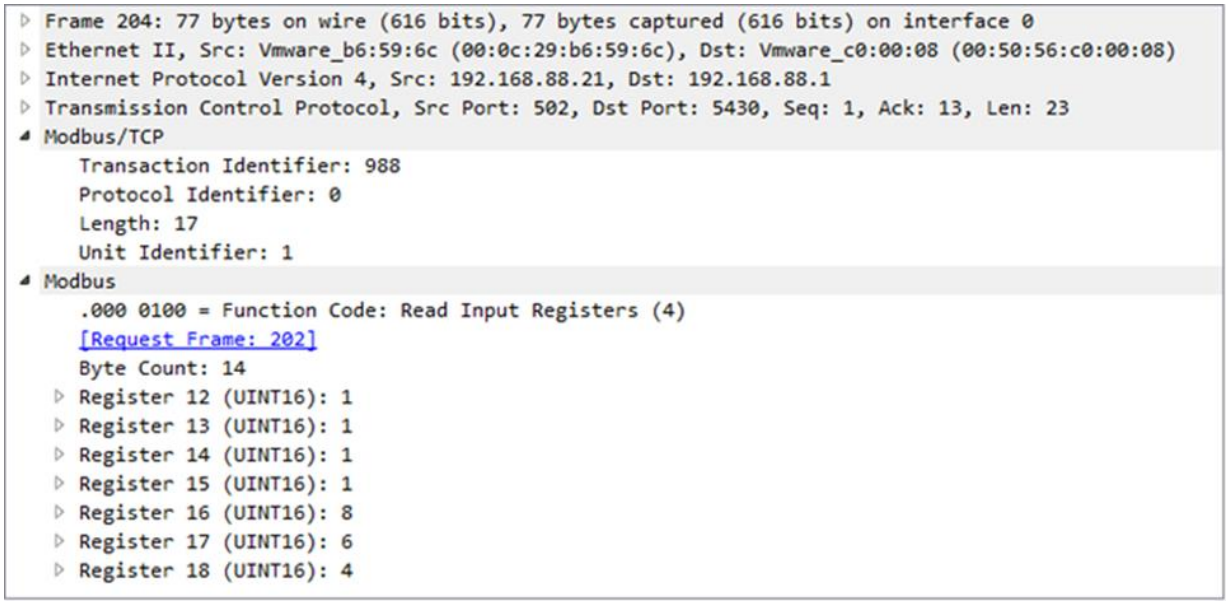
The MITM packet capture attacks were conducted using a Python script which performed an address resolution protocol (ARP) cache poisoning that targeted ScadaBR and PLC 1. This attack let the adversary impersonate both machines and intercept the messages exchanged by them. Figures 5.4a and 5.4b show a request and response generated by ScadaBR and PLC 1 before the ARP cache poisoning. Figure 5.4c shows a request generated by ScadaBR and intercepted by the attacker impersonating PLC 1. Figure 5.4d shows the corresponding response generated by PLC 1 and intercepted by the attacker impersonating ScadaBR.

For the packet injection attacks, we used another Python script to send Modbus commands from the attacker's machine to PLC 1. Figure 5.5a shows one request generated by the attacker to set to DISABLE the operation mode of the traffic light (function code Write Single Coil and database

point reference number 3). Figure 5.5b shows the response generated by PLC 1 confirming the setting of the database point value.

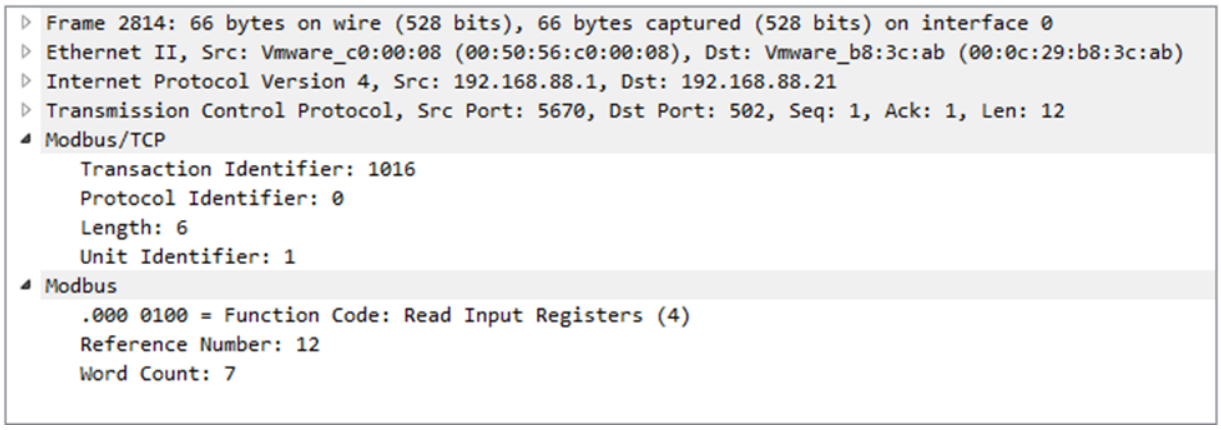


(a) Request sent by ScadaBR to PLC 1 in normal conditions

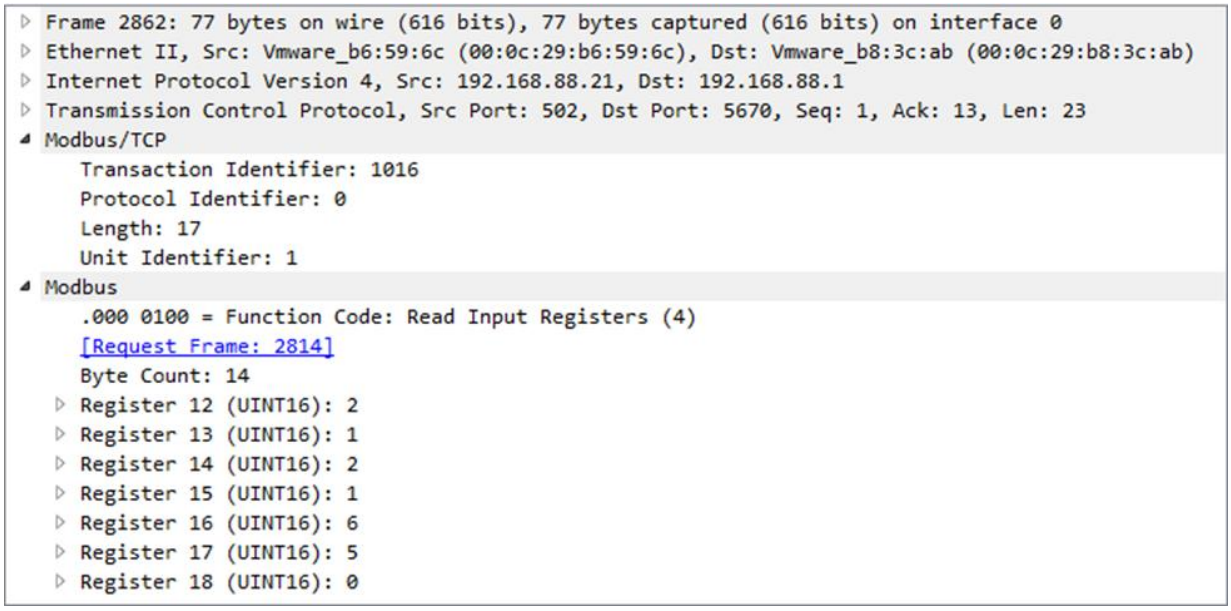


(b) Response from PLC 1 to ScadaBR in normal conditions

Figure 5.4 (part 1): Messages exchanges by ScadaBR and PLC1 in normal conditions and during the MITM attack

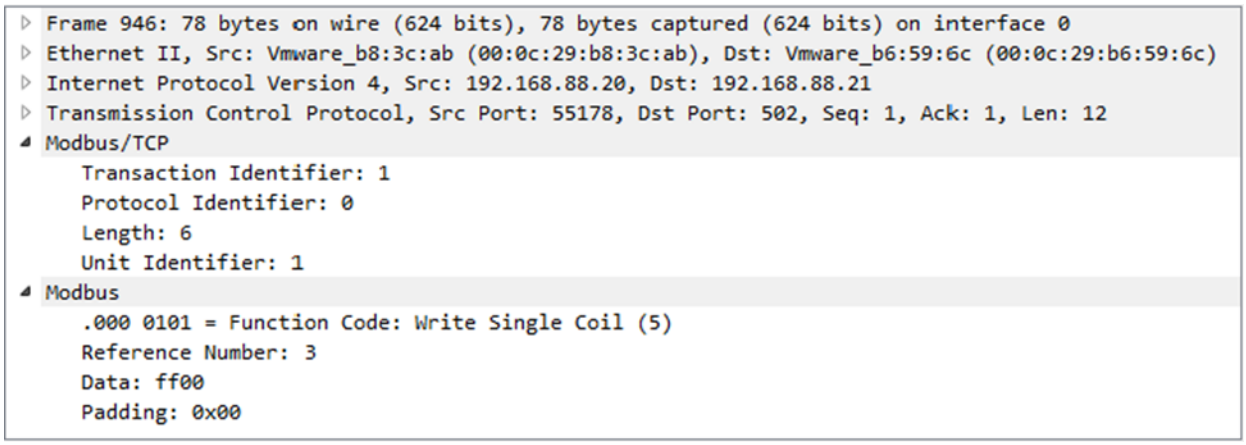


(c) Request sent by ScadaBR and intercepted by the attacker (mac address 00:0c:29:b8:3c:ab) impersonating PLC 1 during the MITM attack

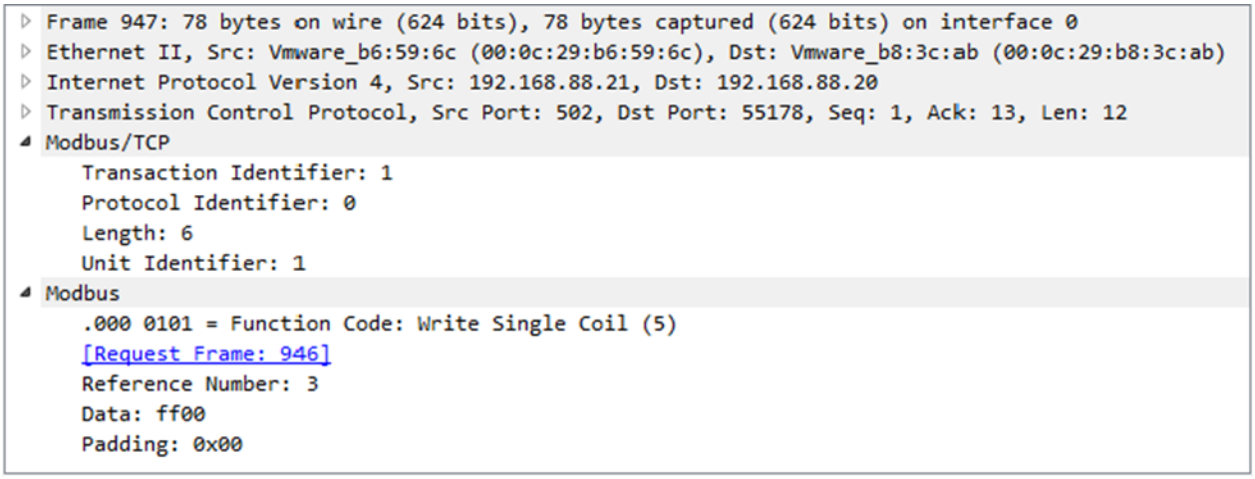


(d) Response sent by PLC 1 and intercepted by the attacker impersonating ScadaBR during the MITM attack

Figure 5.4 (part 2): Messages exchanges by ScadaBR and PLC1 in normal conditions and during the MITM attack



(a) Request sent by the attacker to PLC 1 to set to DISABLE the operation mode of the traffic light



(b) Response sent by PLC 1 confirming the setting

Figure 5.5: Messages exchanged during the packet injection attack

5.6.2 Experimental setup

Going further, we decided to reproduce a cyber attack targeting a coordinated traffic light system. To do that, we recreated the same road corridor used by Ernst and Michaels [84] (Figure 5.6). It is composed of six coordinated signalized intersections, spaced 100 m each. An additional intersection was placed at 2,000 m from the east entry of the corridor to generate vehicle platoons. As in Ernst and Michaels' network, no turns are allowed and there is only one lane in each direction on each road in order to keep the model simple. Nonetheless, it is complex enough to demonstrate the impacts of the attacks on a corridor of signalized intersections. The corridor was coordinated

to favor the eastbound flow using the simulation parameters shown in Table 5.1. The traffic lights operation was configured with the timing plan parameters shown in Table 5.2.

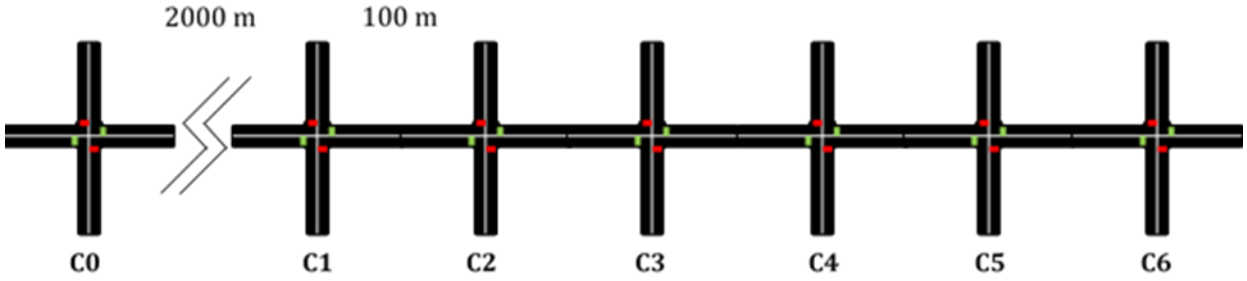


Figure 5.6: Road network used in the experimental setup

Table 5.1: Traffic simulation parameters for the different flows

Parameter	**Eastbound flow**	**Westbound flow**	**Southbound flow**	**Northbound flow**
Max Speed	16.67 m/s	16.67 m/s	11.11 m/s	11.11 m/s
Acceleration	4.5 m/s^2	4.5 m/s^2	4.5 m/s^2	4.5 m/s^2
Deceleration	0.8 m/s^2	0.8 m/s^2	0.8 m/s^2	0.8 m/s^2
Length	5 m	5 m	5 m	5 m
Min Gap	2.5 m	2.5 m	2.5 m	2.5 m
Sigma	0.5	0.5	0.5	0.5
Demand	1000 veh/h	500 veh/h	200 veh/h	200 veh/h
Car following model	Krauss	Krauss	Krauss	Krauss

Table 5.2: Timing plan parameters for coordinated corridor

Cycle length	**Main road green duration**	**Side road green duration**	**Yellow duration**	**All red duration**
98 s	60 s	20 s	6 s	3 s

In order to achieve coordination in the corridor, intersection C1 was chosen as the master intersection of the system, and intersections C2 through C6 were coordinated with offsets of 5.8 s, 11.6 s, 17.4 s, 23.2 s and 29 s respectively. Then, we configured one PLC to control intersection C1 and another PLC to control intersection C5 which was the target of the attacks. In this experiment, the control logic for the four remaining intersections (C2, C3, C4 and C6) were implemented by using the corresponding functionalities within SUMO rather than a simulated PLC. This decision not to use fine-grained emulation for those intersections was only made in order to limit the computer resources required for this experiment. This is without loss of generality, as nothing, other than computational power, would prevent virtualize them all if required.

After configuring the corridor, we executed packet injection attacks targeting signalized intersection C5. Using a Kali Linux machine and the script we used in the validation setup, we sent Modbus/TCP messages to change the programming of traffic lights at the intersection. More specifically, the main green time was changed to 22 s and the side green time to 10 s.

5.7 Experimental results

Attacks impacts were measured in terms of travel time and queue length. First, we recorded each vehicle's travel time for the main corridor in the eastbound direction (going through all intersections). Then, we plotted it as a function of the vehicle number (in the order of their generation at the network entrance). Queue lengths were measured at each simulation step, and reported for each intersection. Travel time results are presented for two simulations, along with the queue lengths over time for four intersections for a given simulation, in Figures 5.7 and 5.8.

As we see, travel time increases two to threefold under attack. Queue lengths increase even more: they are almost non-existent under normal conditions (up to two vehicles for most intersections) and increase four to fivefold (up to 11 vehicles). The effect on queue length is larger for intersections in the middle of the corridor, with queue spillback from downstream intersections. The evaluation of the impact of this simple attack demonstrates that our co-simulation approach can be used to evaluate the physical impact of real cyber attacks (no need to rely on assumptions of the effect of cyber attacks on control components as in the work by Ernst and Michaels [18]).

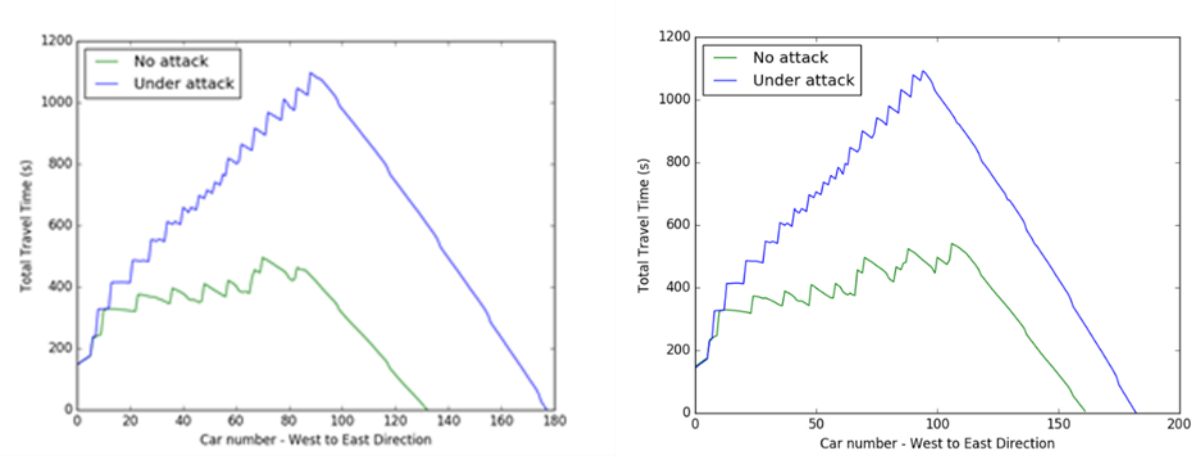


Figure 5.7: Eastbound vehicle travel time for each vehicle for two simulation runs

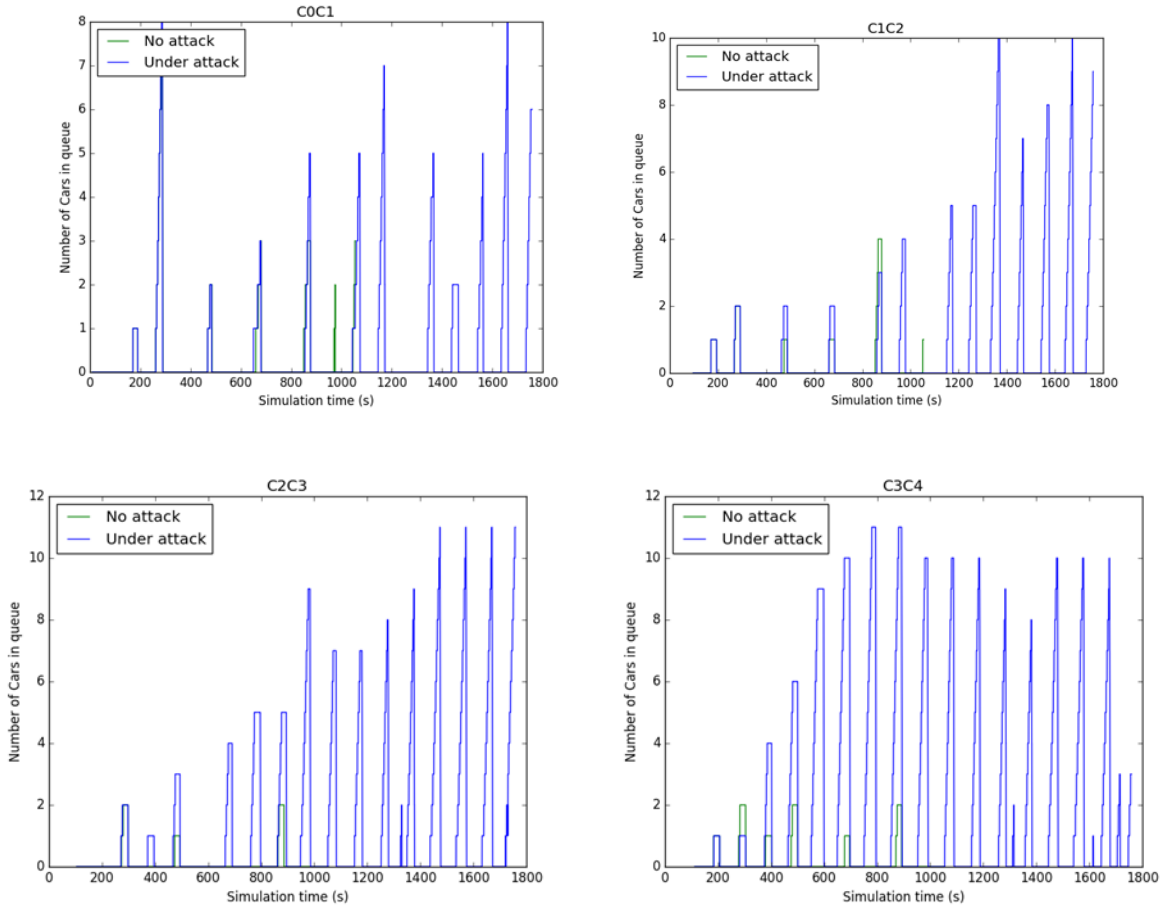


Figure 5.8: Queue length as a function of time for 4 eastbound approaches of the 6 intersections. Results under normal conditions (no attack) are plotted in green, while results under attack are plotted in blue

5.8 Conclusion

We have developed an experimental scenario that successfully integrates a microscopic traffic simulation (SUMO) with an emulated SCADA system (ScadaBR) to reproduce a traffic signal control system for a coordinated corridor of signalized intersections. This test bed has proven to be suitable to evaluate the impact of cyber attacks on traffic control systems. The impact can be measured using traffic performance measures such as travel time and queue length rather than IT performance metrics. For example, in our simple attack scenario, travel time is increased two to threefold and queue length four to fivefold. Moreover, we observed that the physical impact of compromising a single node could be felt at other intersections in the network. Such a result

highlights the importance of understanding the larger impacts of cyber attacks targeting road networks. This type of emergent result could have only been observed in a co-simulation framework (even for our simple scenario) like ours.

The need to use such an approach in more complex road networks is important as it paves the way to more precise quantitative evaluation of the social, economic and environmental impacts of cyber attacks. This can then provide guidance to policy makers to prioritize cyber security efforts. For example, the co-simulation could be used to identify the intersections with the highest impact on traffic (if attacked) to prioritize monitoring efforts.

Our next step is to use our framework to evaluate the resilience of existing highly complex road networks to cyber attacks. This includes implementing and evaluating the impact of more advanced cyber attacks targeting the centrally-controlled traffic control systems, where the impact of the attack could not be evaluated by using traffic simulators alone.

CHAPITRE 6 ASPECTS MÉTHODOLOGIQUES ET RÉSULTATS COMPLÉMENTAIRES

Le chapitre précédent, constitué par l'article « A cyber-physical test bed to measure the impacts of cyber attacks in urban road networks », a décrit le banc d'essai que nous avons développé afin de mesurer les impacts des attaques informatiques contre les réseaux routiers. Comme nous l'avons expliqué au chapitre 4, la démarche montrée dans l'article nous a permis d'atteindre deux des objectifs spécifiques de cette recherche, qui sont : développer un scénario expérimental pour reproduire un système contrôlant le trafic dans des réseaux routiers, et reproduire expérimentalement des attaques informatiques sur les contrôleurs de feux de circulation d'un réseau routier. Il reste deux objectifs spécifiques énoncés au début de la recherche : reproduire expérimentalement l'état de la circulation dans un réseau routier de Montréal, et mesurer les coûts économiques des attaques. C'est pour cela que nous avons configuré un troisième scénario afin d'atteindre ces deux objectifs. Les détails de la démarche complémentaire empruntée et les résultats obtenus sont montrés dans ce chapitre.

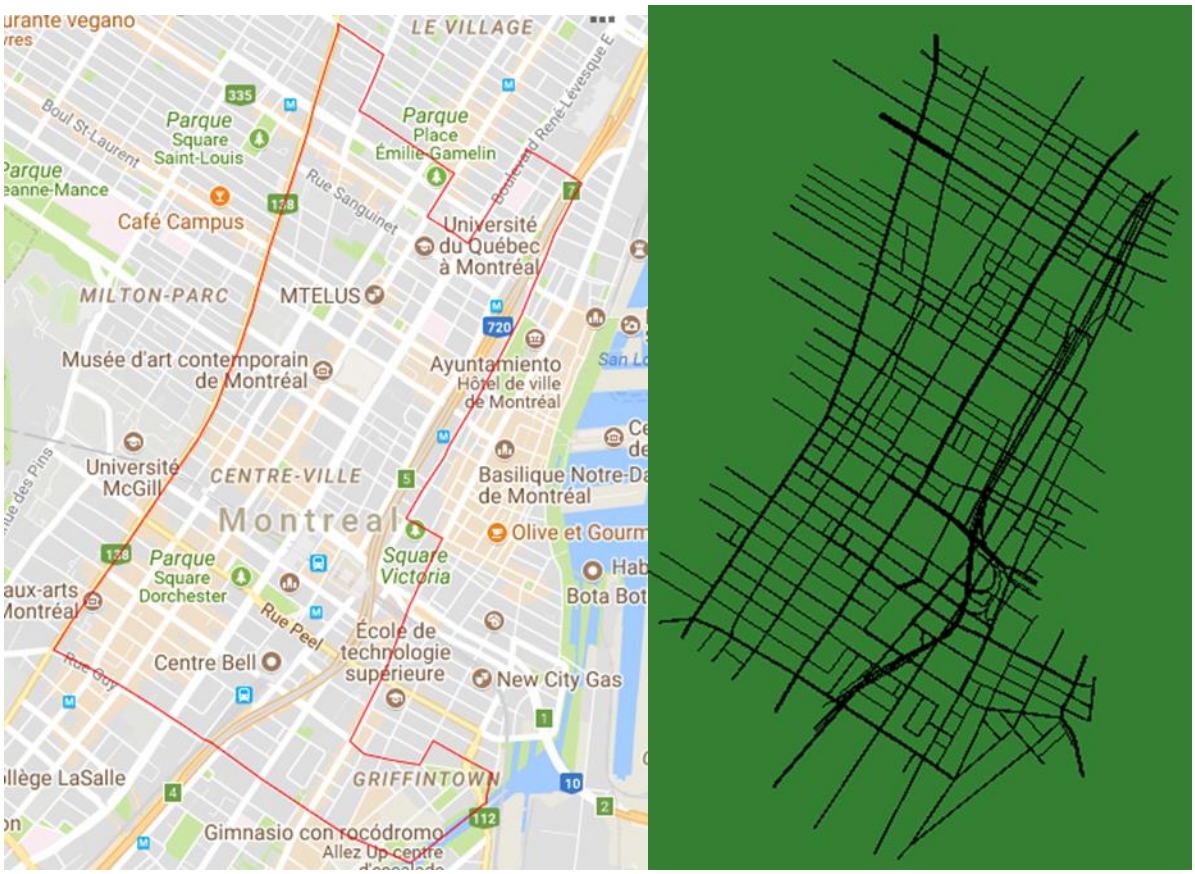
6.1 Attaques informatiques sur un réseau routier de Montréal

Dans cette étape complémentaire, nous avons choisi de mesurer l'impact d'attaques informatiques sur les carrefours à feux du réseau routier du secteur municipal 101 (SM 101) de la Ville de Montréal (Figure 6.1a), qui correspond au Centre-Ville et à la principale concentration de lieux de travail à Montréal. Il occupe une aire approximée de 4 km^2, limitée à l'ouest par la Rue Guy, au nord par la Rue Sherbrooke Ouest, à l'est par une partie des rues Amherst, Saint-Hubert et Saint-Denis, et au sud par une partie des rues Saint-Antoine Ouest, Notre-Dame Ouest, De la Montagne et Murray.

Cette nouvelle démarche a été composée par deux étapes : 1) configurer le réseau et le trafic routier dans SUMO, et 2) exécuter les attaques et mesurer les impacts. Les détails tant de la configuration de la simulation que des résultats obtenus sont présentés aux sous-sections suivantes.

6.1.1 Construction du réseau routier dans SUMO

La démarche a commencé par la construction du réseau routier du SM 101 dans SUMO. Pour ce faire, nous avons téléchargé la carte du SM 101 depuis OpenStreetMap[4], et nous l'avons convertie dans un format lisible par SUMO en utilisant l'application NETCONVERT qui est intégrée au paquet de simulation.



(a) (b)

Figure 6.1 : (a) Carte du secteur municipal 101 de la Ville de Montréal, (b) Réseau routier du secteur municipal 101 de la Ville de Montréal généré par SUMO

[4] OpenStreetMap (OSM) est un projet collaboratif visant à créer une carte modifiable gratuite du monde [95]

Après avoir ouvert le réseau routier avec SUMO, nous avons fait des ajustements requis pour avoir un réseau le plus vraisemblable et simple possible. À cette étape, nous avons vérifié et ajusté le nombre de voies par rue, la vitesse maximale par rue, les virages interdits aux carrefours, entre autres paramètres importés d'OpenStreetMap. Le résultat est le réseau routier montré à la Figure 6.1b.

6.1.2 Configuration de la demande du trafic et la programmation des feux de circulation

L'étape suivante est de configurer la demande du trafic et la programmation des feux de circulation dans la simulation. L'information concernant la demande du trafic a été obtenue sous la forme d'une matrice Origine-Destination[5] (matrice O-D) grâce à la collaboration de la Chaire Mobilité de Polytechnique Montréal. La matrice O-D a été construite à partir des données recueillies dans l'Enquête Origine-Destination de la région métropolitaine de Montréal réalisée en 2013 [88]. Les origines et les destinations sont les zones d'analyse de trafic (« trafic assignement zones », TAZ) utilisées par le ministère des transports. La matrice O-D contenait les déplacements ayant leur origine et/ou leur destination dans le SM 101 et les déplacements traversant le secteur (ceux dont ni leur origine ni leur destination ne se trouvait à l'intérieur du secteur), effectués entre la période de temps de 08h00 à 09h00 d'une journée ouvrable. Elle n'inclut pas les déplacements des piétons, des cyclistes, des personnes se déplaçant en transport en commun (les autobus), des véhicules commerciaux (camions), ni les déplacements des personnes non-résidentes dans la région de Montréal.

Nous avons utilisé l'application OD2TRIPS[6] intégrée à SUMO pour générer les déplacements à partir de la matrice O-D. Nous avons ensuite comparé le nombre de véhicules générés avec de

---

[5] Une matrice Origine-Destination (matrice O-D) est un tableau qui contient *n* lignes et *m* colonnes correspondant aux zones d'origine et destination des déplacements. L'élément placé à la ligne *i* et la colonne *j* indique le nombre de déplacements dont leur origine est la zone *i* et leur destination est la zone *j*. L'information contenue dans les matrices O-D est calculée pour des périodes de temps déterminées (24 h, 1 h, 30 min, de 12h00 à 13h00, etc.) [94].

[6] L'application OD2TRIPS prend l'information contenue dans les matrices O-D et la convertie en déplacements individuels entre des routes spécifiques du réseau (« trips ») ou en flux de véhicules entre les TAZ (« flows »), distribués

vraies valeurs des comptages des véhicules disponibles sur le Portail données ouvertes de la Ville de Montréal. Les résultats de la comparaison ont montré que le comptage résultant des simulations était moindre que celui fait par la Ville de Montréal, dans des intersections évaluées, pour la même période de la journée. Alors, nous avons choisi de doubler la demande du trafic afin de la rendre plus proche de la demande réelle. Finalement, OD2TRIPS a généré environ 37 000 déplacements pour la période de temps simulée.

Quant à la programmation des feux de circulation du réseau routier du SM 101, cette information nous a été fournie par la Ville de Montréal, et nous l'avons intégrée à la simulation en utilisant l'application d'édition des réseaux, NETEDIT, de SUMO.

6.1.3 Paramètres généraux de configuration de la simulation et modèles utilisés

Voici la liste et la description des paramètres utilisés pour configurer la simulation :

- --*begin*, indique l'heure de début de la simulation en secondes. Dans notre cas, nous avons simulé la période de temps de 08h00 à 09h00, donc l'heure de début a été fixée à 28 800.
- --*collision.action*, indique les actions que SUMO exécute à l'occurrence de collisions durant la simulation. Les options disponibles sont : aucune action, afficher un message, téléporter les voitures collisionnées à une autre place du réseau ou les enlever de la simulation. Nous avons sélectionné l'affichage de messages.
- --*departLane*, détermine la voie à laquelle les véhicules sont insérés. OD2TRIPS a attribué la valeur « free » a ce paramètre, qui signifie que les véhicules sont insérés dans la voie la plus disponible (la moins occupée) du tronçon (« edge ») d'origine.
- --*departSpeed*, détermine la vitesse à laquelle les véhicules sont insérés dans la simulation. Nous avons attribué la valeur « random » à ce paramètre, ce qui signifie que la vitesse de départ des véhicules est une valeur entre zéro (0) et la vitesse maximale de la voie où ils sont insérés.

---

sur la période de temps indiquée à la matrice O-D [89]. Chaque déplacement représente un véhicule qui se meut entre deux points du réseau routier.

- --*device.rerouting.with-taz*, signifie que les véhicules peuvent changer d'itinéraire, une fois générés dans la simulation, pour arriver à leur destination. Cela permet d'assurer que les déplacements de toutes les paires OD peuvent être effectués dans le réseau (le choix d'itinéraire est alors validé par SUMO).
- --*duration-log.statistics*, active la génération des statistiques du comptage des voitures et des déplacements à la fin de chaque simulation. Les statistiques du comptage des voitures incluent, pour chaque simulation, le nombre total de voitures générées, le nombre de voitures insérées dans le réseau, le nombre de déplacements complétés, c'est-à-dire, le nombre de voitures qui sont arrivées à leur destination, et le nombre de voitures qui n'ont pas été insérées dans le réseau. Les statistiques des déplacements incluent la longueur moyenne des routes, le temps moyen de parcours, le temps moyen d'attente, le temps moyen perdu et le retard moyen de départ.
- --*end*, indique l'heure de fin de la simulation en secondes. Ce paramètre a été fixé à 32 400, qui corresponde à 09h00.
- --*seed*, initialise le générateur de nombres aléatoires à partir de la valeur donnée. SUMO utilise un générateur de nombres aléatoires (« random number generation », RNG) pour plusieurs variables, comme les intervalles entre les instants d'apparition des véhicules, les vitesses des véhicules, etc. Nous avons attribué une valeur différente (choisie aléatoirement) à ce paramètre pour chaque simulation.
- --*step-length*, définie la durée des pas simulation en secondes. Nous avons fixé la valeur de ce paramètre à 0,1.
- --*tripinfo-output*, produit un fichier à la fin de chaque simulation contenant l'heure de départ, l'heure d'arrivée, le temps perdu, le temps de parcours, le temps d'attente, entre autres métriques, des véhicules qui ont complété leurs déplacements.

SUMO utilise des générateurs de nombres aléatoires et des modèles microscopiques pour reproduire le comportement des conducteurs :

- Génération de nombres aléatoire. SUMO utilise un algorithme pseudo-aléatoire pour la génération de nombres aléatoires. La séquence des nombres générée dépend d'une valeur d'initialisation (« seed »). SUMO utilise deux instances différentes pour la génération de

nombres aléatoires : une pour la création des véhicules et l'autre pour le comportement dynamique (modèles microscopiques).

- Distribution des vitesses. Par défaut, les véhicules dans la simulation se déplacent à la vitesse maximale attribuée à la voie sur laquelle ils circulent. Cependant, SUMO permet de modifier ce comportement en utilisant le paramètre *speedFactor* lors de la génération des véhicules. La vitesse maximale des véhicules est le produit de la vitesse maximale de la voie sur laquelle le véhicule se déplace avec la valeur attribuée à *speedFactor*.
- Modèle de suivi des véhicules (« car following model »). Ce modèle détermine la vitesse de circulation des véhicules en relation avec le véhicule qui le précède. Le modèle de suivi de véhicule utilisé dans les simulations est le modèle de Krauss [89], qui est le modèle par défaut dans SUMO. Il repose sur le déplacement des véhicules à une vitesse aussi élevé que possible tout en maintenant une conduite sécuritaire, c'est-à-dire, en évitant des collisions si le véhicule devant eux commence à freiner.
- Modèle de changement de voie (« lane-changing model »). Ce modèle détermine le choix de voie sur les routes à plusieurs voies et fait les ajustements de la vitesse lors d'un changement de voie. Le modèle utilisé par défaut est le modèle de Jakob Erdmann [90].
- Modèle des intersections (« intersection model »). Ce modèle détermine le comportement des conducteurs aux différents types d'intersections, par rapport aux règles de droit de passage, le respect des écarts et l'évitement du blocage de l'intersection.

6.1.4 Détermination du nombre de simulations à exécuter

Pour déterminer le nombre de simulations différentes à exécuter (avec différentes valeurs initiales pour les générateurs de nombres aléatoires) afin de garantir la représentativité des résultats obtenus des simulations, nous avons adopté la méthode de stabilisation de la valeur de la fonction objectif décrite par Gauthier en [91]. Dans notre cas, nous utilisons le temps perdu qui est la métrique de performance que nous avons choisie pour mesurer l'impact des attaques contre les feux de circulation du réseau routier du SM 101 de la Ville de Montréal, présentées dans ce chapitre.

50 simulations ont été effectuées pour les conditions normales du trafic dans le réseau. Nous avons calculé le temps perdu moyen pour chacune des 50 simulations et nous avons construit une première série de données contenant les 50 valeurs obtenues. Nous avons ensuite généré une

deuxième série de données dont la i-ème valeur a été la moyenne des i premiers temps perdus moyens des simulations 1 à i. Finalement, le nombre de simulations à exécuter est la valeur à partir de laquelle la valeur moyenne du temps perdu moyen se stabilise. Le graphique de la Figure 6.2 montre que la valeur moyenne du temps perdu moyen se stabilise à partir de 20 simulations, qui est donc le nombre de simulations pour chacun des tests effectués.

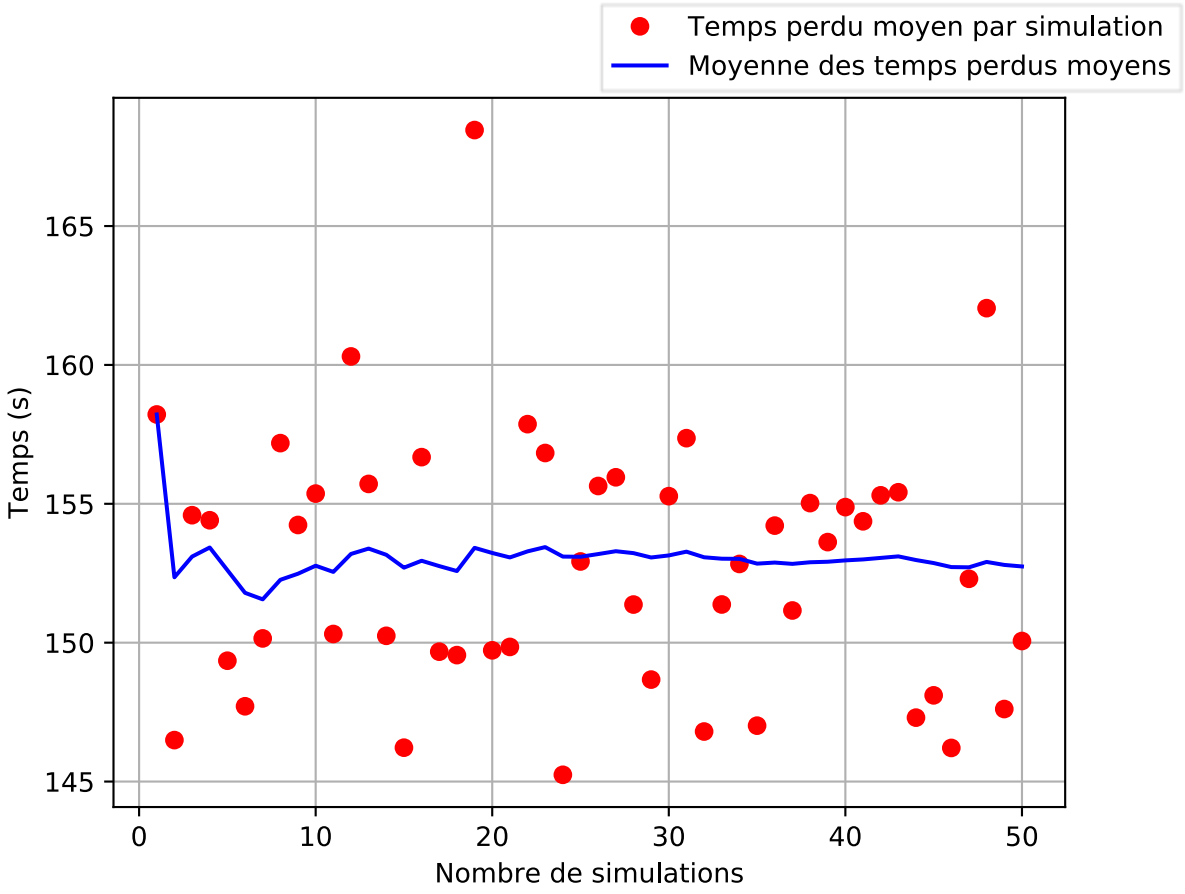


Figure 6.2 : Moyenne des temps perdus moyens par simulation en fonction du nombre de simulation

6.1.5 Détermination du temps d'initialisation

Le temps d'initialisation d'une simulation de la circulation est le temps nécessaire pour que la circulation sur le réseau atteigne un état stationnaire. Cela revient à ne pas prendre en compte des observations du début de la simulation, lorsque les véhicules sont les premiers sur le réseau et rencontrent donc des conditions de circulation différentes des conditions stationnaires du réseau,

par exemple en termes de présence d'autres véhicules sur le réseau qui vont causer de la gêne et des retards (files d'attente).

Pour déterminer le temps d'initialisation, nous avons regardé le rythme de sortie des véhicules dans le réseau. Spécifiquement, pour les conditions normales, nous avons construit le graphique du nombre cumulé de véhicules ayant complété leur déplacement dans chaque simulation en fonction de leur heure d'arrivée à destination. Dans le graphique, nous avons identifié l'instant de la simulation à partir duquel la tangente à la courbe devient constante. La Figure 6.3 montre qu'à partir de 29 000 secondes, la courbe du nombre cumulé de véhicules devient une droite. Le temps d'initialisation de nos simulations est donc constitué des 200 premières secondes. Les résultats présentés dans ce chapitre ne prennent en compte que les valeurs du temps perdu des déplacements complétés dont l'heure d'arrivée est supérieure à 29 000 secondes.

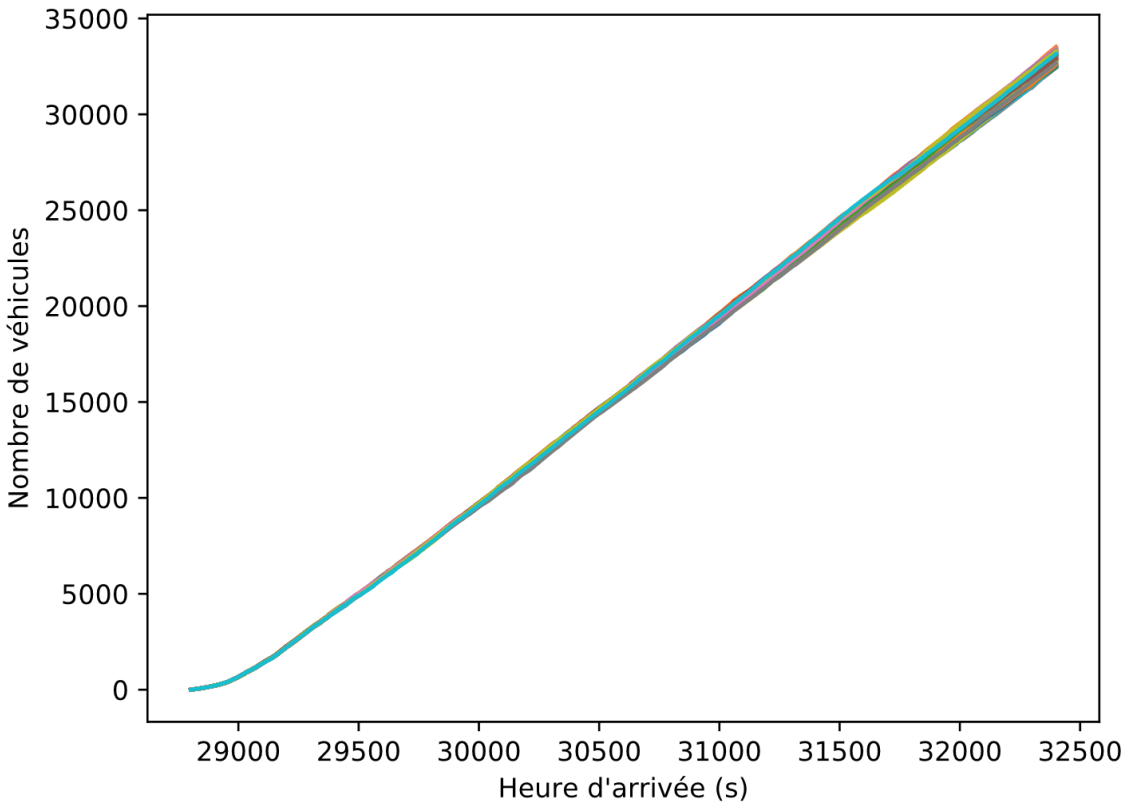


Figure 6.3 : Nombre cumulé de véhicules ayant complété leur déplacement dans chaque simulation en fonction de leur heure d'arrivée à destination

6.1.6 Métriques utilisées

Le dernier objectif spécifique de notre recherche consiste à mesurer les coûts économiques des attaques informatiques en fonction du retard global résultant des attaques sur le réseau. Dans SUMO, la métrique qui représente ce retard est le temps perdu. Celui-ci est définit comme le temps de parcours supplémentaire que subissent les conducteurs en raison de se déplacer à une vitesse inférieure à la vitesse idéale de circulation (la vitesse à laquelle ils se déplaceraient s'il n'y avait pas de congestion dans le réseau). Cette métrique est contenue dans les fichiers *tripinfo* générés à la fin de chaque simulation.

Aussi, nous avons analysé les statistiques des comptages des véhicules, produites à la fin de chaque simulation, afin de connaître le comportement du trafic dans le réseau pendant les simulations.

6.2 Attaques exécutées et résultats obtenus

Pour attaquer les feux de circulation du SM 101 nous avons choisi d'exécuter des attaques d'injection de paquets visant à altérer l'opération normale des feux de circulation de deux façons différentes qui sont : 1) désactiver les feux de circulation, et 2) modifier les plans des feux. De plus, nous avons utilisé deux stratégies pour sélectionner les victimes des attaques : a) sélection aléatoire, et b) sélection ciblée. Finalement, après avoir établi les types d'attaque à exécuter et les stratégies de sélection des victimes, nous avons lancé les attaques présentées dans les sous-sections suivantes.

Pour les fins de ce mémoire, nous appellerons Attaque 1 les attaques de désactivation des feux de circulation, et Attaque 2 les attaques de modification des plans des feux. Ainsi, nous utiliserons le terme feu de circulation pour faire référence aux carrefours à feux et à l'ensemble des feux contrôlant un même carrefour.

6.2.1 Attaque 1 individuelle contre les feux de circulation du SM 101

Nous avons commencé en lançant une Attaque 1 contre tous les feux de circulation se trouvant dans le SM 101 (185 feux de circulation). Nous avons lancé une simulation pour attaquer un feu de circulation à la fois. Pour cette expérimentation, nous n'avons pas lancé les 20 simulations pour chaque feu de circulation attaqué, car une telle démarche nous prendrait environ de 60 jours pour la compléter.

Après avoir complété les attaques contre tous les feux de circulation du secteur, nous avons calculé le temps perdu moyen pour chaque simulation en fonction du temps perdu enregistré pour tous les déplacements complétés (des véhicules étant arrivés à leur destination) pendant la simulation. Puis, nous avons trié les feux de circulation en fonction de leur valeur de criticité, mesurée par la valeur du temps perdu moyen. Nous avons sélectionné les 50 feux de circulation les plus critiques avec la valeur du temps perdu moyen la plus grande.

6.2.2 Attaque 1 contre groupes de feux de circulation choisis aléatoirement

Après avoir ordonnée chacun des feux de circulation du SM 101 par criticité, nous avons lancé la même attaque, mais cette fois par groupes de feux de circulation choisis aléatoirement. La taille des groupes a varié de 5, 10, 20 et 50 feux de circulation. Nous avons lancé 20 simulations pour chaque taille de groupe et les feux de circulation victimes ont changé d'une simulation à l'autre. La Figure 6.4 montre la distribution des valeurs du temps perdu moyen des 20 simulations selon le nombre de feux de circulation par groupe. Le groupe « 0 » représente les valeurs du temps perdu moyen pour les simulations dans les conditions normales (sans attaque).

Les résultats de cette nouvelle expérimentation montrent que plus le nombre de feux attaqués augmente, plus la valeur du temps perdu moyen diminue, ce qui représente un impact positif. Une fois les feux de circulation sont désactivés, les conducteurs agissent comme s'il y avait des panneaux arrêt sur toutes les approches des carrefours. Dans ce cas, les conducteurs respectent les règles de conduite, qui établissent qu'en face des panneaux arrêt les conducteurs doivent marquer l'arrêt et laisser la priorité aux autres usagers se trouvant déjà au carrefour, avant de continuer leur chemin. Dans une telle situation, le temps d'attente aux carrefours munis de panneaux arrêt pourrait effectivement être moindre que celui aux carrefours à feux. Cependant, le temps d'attente augmenterait dans les cas de piétons traversant les carrefours, mais ce trafic n'a pas été inclus dans les simulations. Cette situation aurait pu favoriser les déplacements dans les simulations et mener à la diminution du temps perdu.

Dans ce contexte, augmenter la capacité d'un attaquant d'attaquer des feux ne se traduit pas par une augmentation de l'impact. En fait, on voit plutôt l'effet contraire.

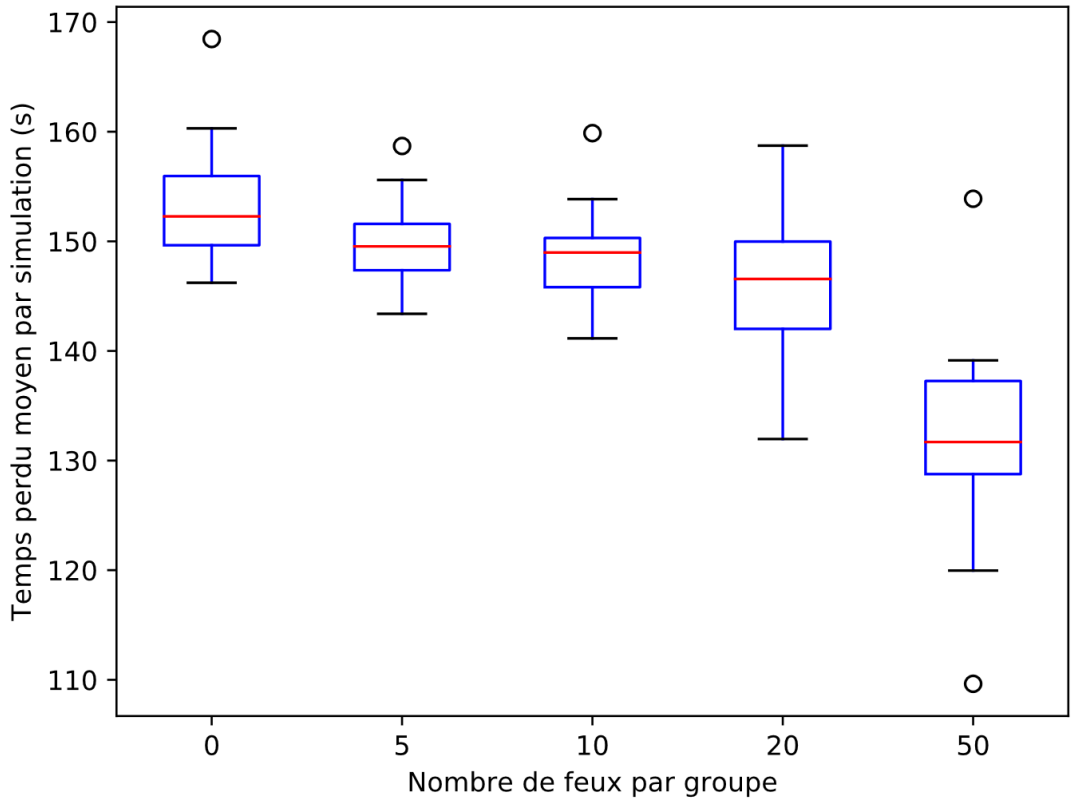


Figure 6.4 : Résultats de l'Attaque 1 contre groupes de feux de circulation choisis aléatoirement

6.2.3 Attaque 1 contre groupes de feux de circulation ciblés

Cette fois, nous avons lancé l'Attaque 1 contre les 50 feux de circulation identifiés comme les plus critiques, selon le critère expliqué à la sous-section 6.2.1. De façon similaire à l'attaque antérieure, nous avons exécuté l'attaque par groupes de feux. Nous avons commencé par attaquer les cinq premiers feux de circulation de la liste, après les dix premiers feux de circulation de la liste, ensuite les premiers 20 feux de circulation de la liste, et finalement nous avons attaqués les cinquante feux de circulation les plus critiques simultanément. Nous avons lancé 20 simulations pour chaque taille de groupe. La Figure 6.5 montre les résultats obtenus pendant cette attaque.

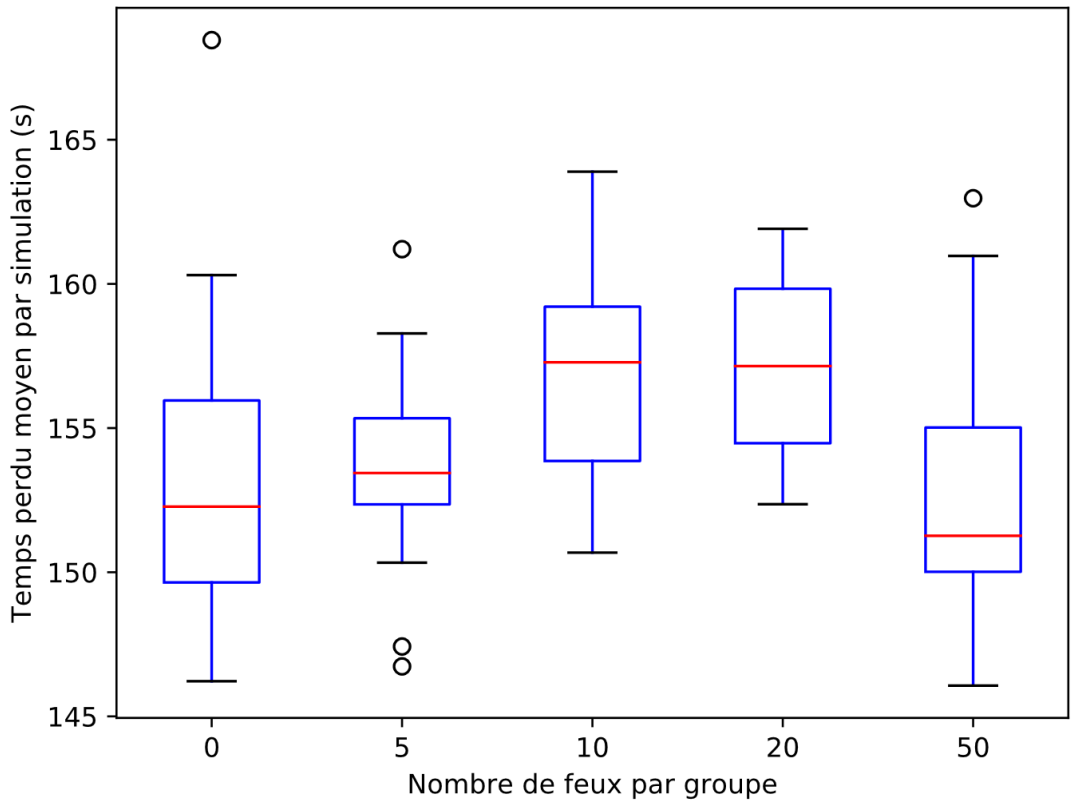


Figure 6.5 : Résultats de l'Attaque 1 contre groupes de feux de circulation ciblés

Les résultats montrent que, par rapport aux conditions normales, le temps perdu moyen pendant l'attaque a augmenté pour les cas de 5, 10 et 20 feux de circulation attaqués, tandis qu'il est revenu à la valeur initiale (dans les conditions normales) pour le cas de 50 feux de circulation attaqués. Par contre, par rapport à l'attaque de feux de circulation sélectionnés aléatoirement (Figure 6.4), le temps perdu moyen pour l'attaque ciblée a été supérieur pour toutes les tailles de groupes de feux attaqués. Ces résultats font ressortir que l'impact des attaques varie selon la stratégie de sélection des victimes. Dans l'attaque antérieure les victimes ont été choisies de façon aléatoire, mais dans cette attaque les victimes ont été choisies en fonction d'une métrique de performance.

6.2.4 Attaque 2 individuelle contre les feux de circulation du SM 101

Ayant lancé l'Attaque 1 tant pour les victimes aléatoires que ciblées, nous avons par la suite lancé l'Attaque 2, qui consiste à modifier le plan de feu des feux de circulation attaqués. Pour toutes les attaques, nous avons doublé la durée du cycle, en doublant la durée de tous les intervalles du plan

de feu. De façon similaire à l'Attaque 1, nous avons attaqué tous les feux de circulation du réseau routier du SM 101, un feu à la fois. Nous avons lancé l'attaque une seule fois contre chacun des feux, et nous avons classé les feux de circulation par rapport au temps perdu moyen obtenu des simulations. Finalement, nous avons identifié les 50 feux de circulation les plus critiques par rapport à la valeur du temps perdu moyen.

6.2.5 Attaque 2 contre groupes de feux de circulation choisis aléatoirement

Cette fois, nous avons lancé l'Attaque 2 par groupes de feux de circulation choisis aléatoirement. Similairement à l'Attaque 1 par groupes aléatoires, nous avons varié la taille des groupes de 5, 10, 20 et 50 feux de circulation, et nous avons lancé 20 simulations pour chaque taille de groupe sélectionnant un nouveau groupe de victimes d'une simulation à l'autre. La Figure 6.6 montre la distribution des valeurs du temps perdu moyen des 20 simulations selon le nombre de feux de circulation par groupe. Le groupe « 0 » représente les valeurs du temps perdu moyen pour les simulations dans les conditions normales (sans attaque).

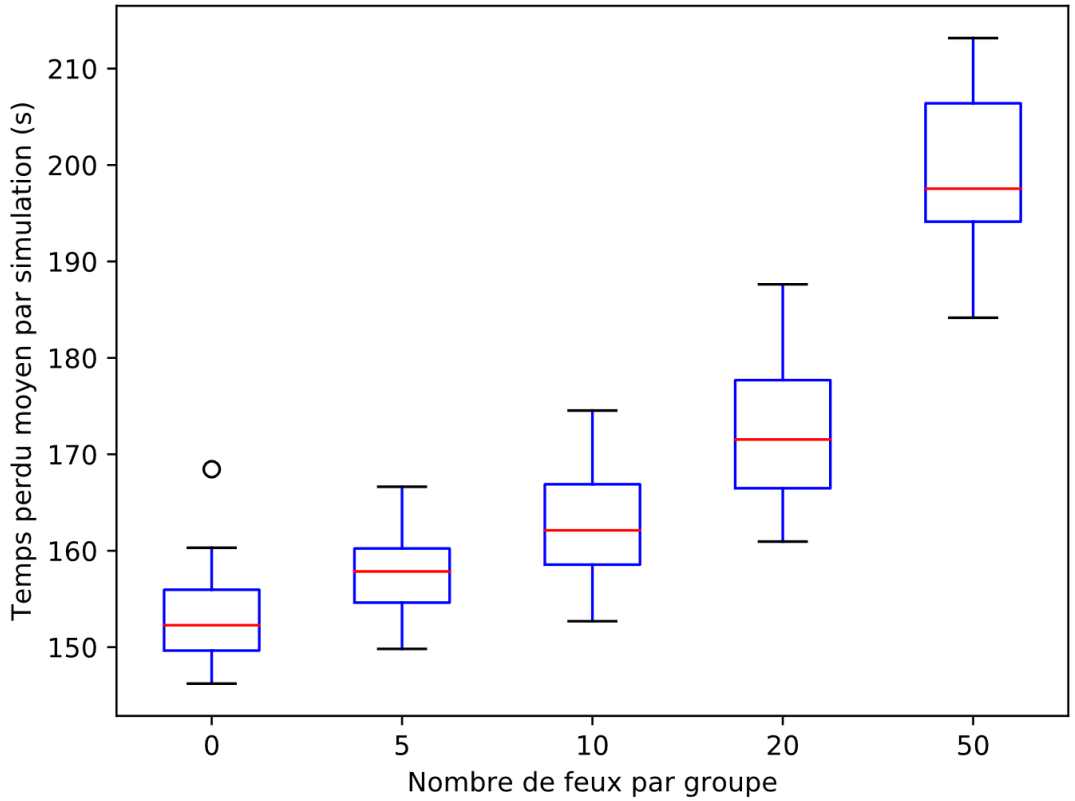


Figure 6.6 : Résultats de l'Attaque 2 contre groupes de feux de circulation choisis aléatoirement

On peut constater que l'Attaque 2 a plus d'impact sur le temps perdu que l'Attaque 1 (désactivation des feux). De plus, les résultats mettent en évidence que le temps perdu moyen augmente au fur et à mesure que le nombre de feux de circulation attaqués augmente. Ceci démontre qu'une augmentation de la capacité de l'attaquant se traduit par un impact plus grand contrairement à ce qui était le cas pour l'Attaque 1. Pour le pire des cas (attaque contre 50 feux de circulation), la moyenne des temps perdus moyens par simulation a augmenté de 30% (de 153,2 à 199,6) par rapport à la moyenne des temps perdus moyens par simulation dans les conditions normales.

6.2.6 Attaque 2 contre groupes de feux de circulation ciblés

Finalement, nous avons lancé l'Attaque 2 contre les 50 feux de circulation identifiés comme les plus critiques. De nouveau, nous avons commencé pour attaquer les cinq premiers feux de circulation de la liste, ensuite les dix feux de circulation de la liste, après les vingt feux de circulation de la liste, et finalement les cinquante feux de circulation de la liste simultanément. Nous avons aussi lancé 20 simulations pour chaque taille de groupe sans changer les victimes d'une simulation à l'autre. La Figure 6.7 montre les résultats obtenus pendant cette attaque.

Dans ce cas, les valeurs du temps perdu moyen ont été toutes supérieures à celles de l'Attaque 2 contre les feux choisis aléatoirement. La moyenne des temps perdus moyens par simulation pour le pire des cas (attaque contre 50 feux) a augmenté de 40% (de 153,2 à 215,36) par rapport aux conditions normales, et a augmenté de 8% (de 199,6 à 215,36) par rapport à l'attaque contre les 50 feux de circulation choisis aléatoirement. Toutes les valeurs sont montrées au Tableau 6.3. Ces résultats renforcent ce que nous avions déjà détecté à partir des résultats de la sous-section 6.2.3 : que les attaques contre les victimes ciblées ont plus d'impact que les attaques contre les victimes sélectionnées aléatoirement.

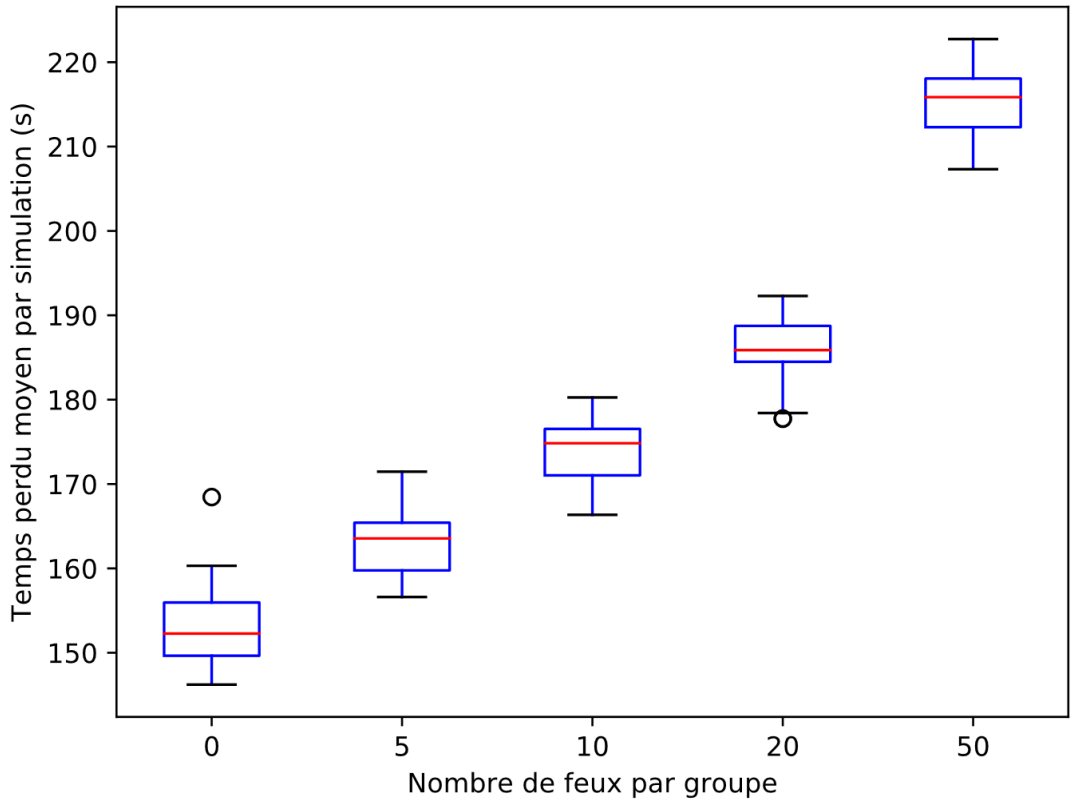


Figure 6.7 : Résultats de l'Attaque 2 contre groupes de feux de circulation ciblés

6.2.7 Comparaison des impacts résultants des attaques

Dans cette section nous faisons une comparaison des impacts générés par les attaques décrites dans les sous-sections précédentes.

Pour commencer, la Figure 6.8 montre la distribution du temps perdu moyen tant pour l'attaque de désactivation des feux de circulation (Attaque 1) que pour l'attaque de modification des plans des feux (Attaque 2) lancées individuellement contre les feux de circulation du SM 101. Cela démontre que l'attaque de modification des plans de feux produit plus d'impact sur le temps de perdu que l'attaque de désactivation des feux.

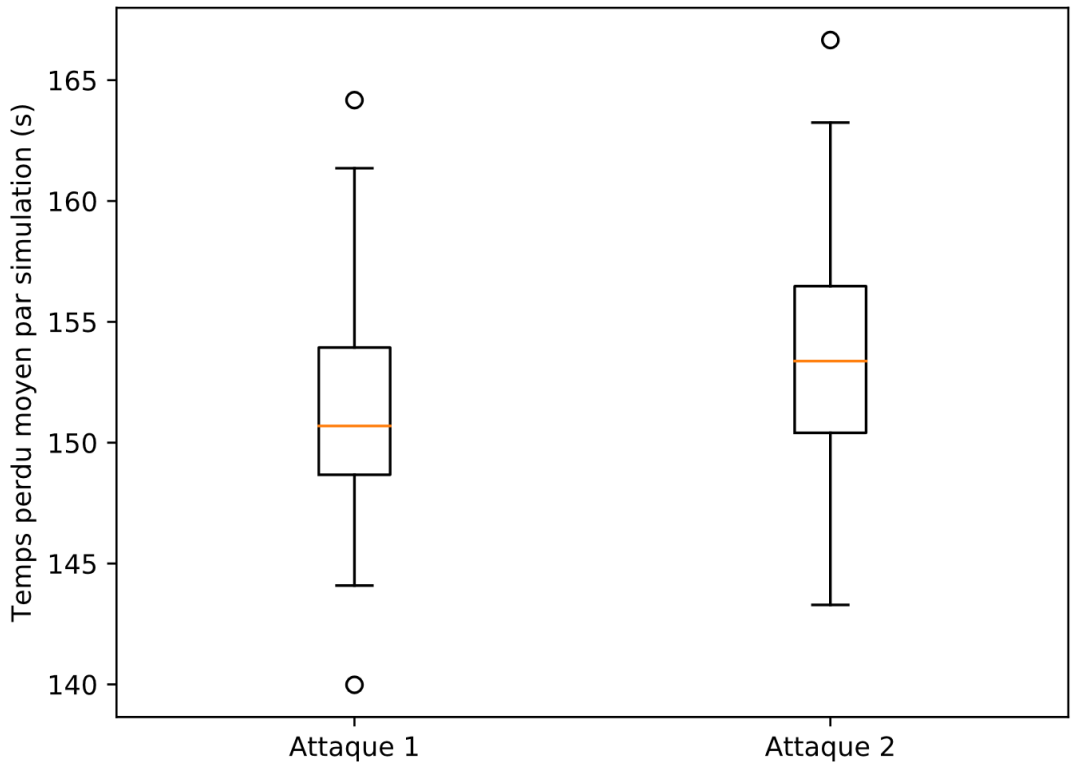


Figure 6.8 : Temps perdu moyen des attaques individuelles contre les feux de circulation

D'une autre part, le Tableau 6.1 contient la valeur moyenne du temps perdus moyens calculée sur l'ensemble de valeurs obtenues par les 20 simulations de chacune des conditions simulées. Ces valeurs sont montrées à la Figure 6.9 afin de pouvoir les comparer de façon visuelle. Cela renforce que l'attaque de modification des plans de feux a plus d'impact que l'attaque de désactivation des feux, mais aussi que les attaques ciblées ont plus d'impact que les attaques où les victimes sont sélectionnées aléatoirement, indépendamment du type d'attaque.

Tableau 6.1 : Moyenne des temps perdus moyens par simulation (en secondes) pour les conditions normales et pour les attaques lancées contre groupes de feux de circulation

		Attaque 1		***Attaque 2***	
Conditions normales	**Nbr. feux**	**Sélection aléatoire**	**Sélection ciblée**	**Sélection aléatoire**	**Sélection ciblée**
153,20	5	149,47	153,67	157,47	163,14
	10	148,68	156,90	162,52	174,12
	20	145,99	157,16	172,56	185,89
	50	132,17	152,69	199,60	215,36

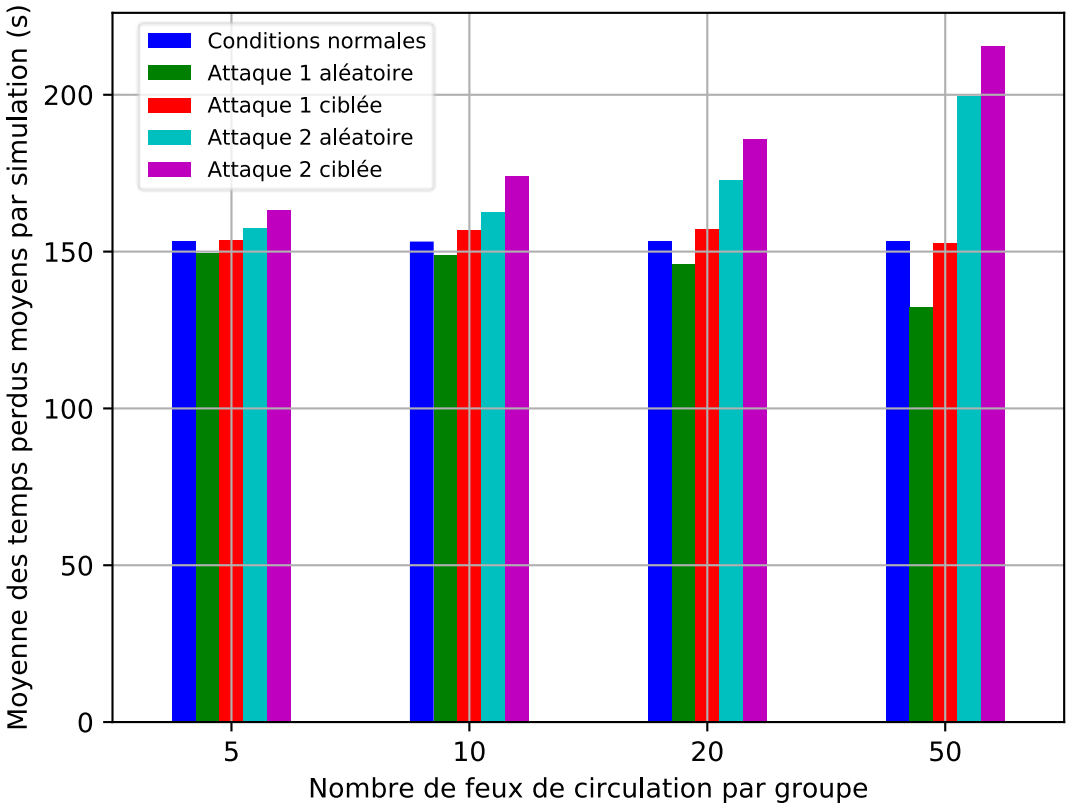


Figure 6.9 : Moyenne des temps perdus moyens en conditions normales et pendant les attaques contre groupes de feux de circulation

Finalement, les tableaux 6.2 et 6.3 montrent les statistiques du comptage de voitures, tant pour les conditions normales que pour les attaques contre groupes de feux de circulation. D'après ces valeurs, il est évident que les attaques ont aussi impacté les conditions de la circulation dans le réseau. Par exemple, pour les attaques de modification des plans de feux (Attaque 2) le nombre de véhicules en déplacement, de véhicules qui n'ont pas été insérés dans la simulation et de véhicules téléportés ont été toujours supérieures aux valeurs obtenues pendant les attaques de désactivation des feux (Attaque 1). Conséquemment, pour les attaques de modification des plans des feux le nombre de déplacements complétés et le nombre de voitures insérées dans la simulation ont été moindres que les valeurs obtenues pour les attaques de désactivation des feux. Ces résultats correspondent au comportement du temps perdu moyen montré pour chacune des attaques, et ils mettent en évidence que plus le réseau est congestionné, plus le temps perdu par les automobilistes

augmente et plus ils sont nombreux à ne pas atteindre leur destination dans le temps fixe de la simulation.

Tableau 6.2 : Statistiques des nombres de véhicules pour l'Attaque 1 contre groupes de feux de circulation

		Sélection aléatoire				***Sélection ciblé***			
	Normal	**5**	**10**	**20**	**50**	**5**	**10**	**20**	**50**
Déplacements générés	37 032	37 032	37 032	37 032	37 032	37 032	37 032	37 032	37 032
Véhicules insérées	36 413	36 490	36 531	36 554	36 819	36 490	36 440	36 461	36 685
Déplacements complétés	32 990	33 152	33 242	33 315	33 882	32 939	32 939	33 041	33 411
Véhicules en déplacement	3 423	3 338	3 289	3 239	2 937	3 551	3 501	3 420	3 274
Véhicules non insérés	619	542	501	478	213	542	592	571	347
Véhicules téléportés	47	36	39	46	41	51	66	67	76

Tableau 6.3 : Statistiques des nombres de véhicules pour l'Attaque 2 contre groupes de feux de circulation

		Sélection aléatoire				***Sélection ciblé***			
	Normal	**5**	**10**	**20**	**50**	**5**	**10**	**20**	**50**
Déplacements générés	37 032	37 032	37 032	37 032	37 032	37 032	37 033	37 032	37 032
Véhicules insérés	36 413	36 334	36 168	35 945	35 270	36 359	36 108	35 784	34 790
Déplacements complétés	32 990	32 875	32 548	32 124	30 454	32 749	32 139	31 349	29 009
Véhicules en déplacement	3 423	3 459	3 620	3 821	4 816	3 610	3 969	4 435	5 781
Véhicules non insérés	619	698	864	1087	1762	673	925	1 248	2 242
Véhicules téléportés	47	43	51	67	161	40	67	123	301

6.3 Estimation des coûts économiques des impacts

Des études sont faites régulièrement par les autorités municipales, régionales et nationales afin d'estimer les coûts économiques de la congestion dans leurs réseaux routiers. L'information prise en compte pour l'estimation de ces coûts varie d'une étude à l'autre. Cependant, il existe trois éléments qui sont inclus dans les estimations de la plupart de ces études : les retards des usagers, la consommation supplémentaire de carburant et les émissions supplémentaires de polluants et de gaz à effet de serre [2] [1]. Étant donné que nous n'avons pas calibré le modèle de simulation pour reproduire la distribution des véhicules circulant sur les réseaux routiers actuels, tels que les véhicules avec des moteurs à combustion et les véhicules électriques, nous n'avons pas mesuré la

consommation du carburant ni les émissions de polluants et de gaz à effet de serre. Les coûts économiques résultants des attaques lancées contre le réseau de Montréal modélisé ont donc été estimés seulement en considérant le temps perdu. Spécifiquement, nous avons fait l'estimation en tenant compte de la variation du temps perdu par rapport aux conditions normales, du nombre de déplacements complétés pour chaque attaque (montrés dans les tableaux 6.2 et 6.3) et de la valeur monétaire du temps des déplacements.

Le Ministère des Transports, de la Mobilité durable et de l'Électrification des Transports publie régulièrement un guide contenant les paramètres utilisés pour estimer les coûts de ses projets [92]. Dans la guide de l'année 2016, nous avons trouvé la valeur horaire du temps des déplacements pour les véhicules légers (automobiles, fourgonnettes, camionnettes, véhicules utilitaires sport et motocyclettes) qui se montre au Tableau 6.4. La valeur varie selon le motif du déplacement (*Affaires* ou *Autre*) et la nature des occupants (*Conducteur* ou *Passager*).

Tableau 6.4 : Valeur horaire du temps de déplacements des véhicules légers (tiré de [92])

Motif	***Valeur horaire (CAD 2016)***
Affaires	23,63
Autre - Conducteur	13,52
Autre – Passagers	9,50

De plus, le rapport *Évaluation des coûts de la congestion routière dans la région de Montréal pour les conditions de référence de 2008* [2] distingue quatre motifs associés aux déplacements habituels : affaires, travail, études et autres. Les déplacements associés au motif *affaires* sont définis comme les déplacements faits en situation de travail, tels que les rendez-vous d'affaires durant les heures de travail ou les déplacements faits par les chauffeurs, les camionneurs et les personnes qui font des livraisons des biens en conduisant un véhicule pour le faire. Le rapport explique que la valeur horaire du temps pour ce motif et calculé en fonction du salaire brut de l'employé plus des contributions de son employeur. Les déplacements associés au motif *travail* sont définis comme les déplacements aller-retour qui s'effectuent entre le domicile et le lieu de travail. La valeur horaire du temps pour ce motif est calculée comme la moyenne de la valeur du temps d'un déplacement pour le motif *Affaires* et un déplacement pour le motif *Autres*. D'après les valeurs montrées au Tableau 6.4 cela correspond à 18,56 CAD. Les déplacements pour le motif *études* correspondent

aux déplacements effectués par les étudiants en se rendant à leur établissement d'enseignement. Sa valeur corresponde à 25 % de la valeur du temps pour le motif *Affaires*, c'est-à-dire, 5,91 CAD. Finalement, les déplacements associés au motif *Autres*, correspondent aux déplacements effectués pour d'autres activités qui ne sont ni le travail ni les études, telles que les loisirs, le magasinage, les rendez-vous de santé, etc. Sa valeur correspond au revenu horaire net d'un employé, hors d'impôt et de taxes, tel que montré au Tableau 6.4. Les valeurs résultantes sont montrées dans le Tableau 6.5.

D'après le rapport des faits saillants de l'enquête Origine-Destination réalisée à la région métropolitaine de Montréal en 2013 [93], 49 % des déplacements effectués en période de pointe du matin ont été faits pour le motif travail, 28 % ont été faits pour le motif études, 11 % ont été faits pour aller chercher ou déposer quelqu'un[7], et 12 % ont été faits pour un autre motif.

En ce qui concerne l'occupation des véhicules, le même rapport affirme que le taux d'occupation moyen par automobile est de 1,20. Ce taux d'occupation signifie que 100 % des déplacements sont faits par le conducteur et 20 % des déplacements sont faits par un passager.

Le Tableau 6.5 montre les valeurs horaires du temps des déplacements et la distribution des déplacements selon le motif que nous avons utilisées pour estimer les coûts des attaques.

Tableau 6.5 : Valeurs horaires du temps de déplacements utilisées pour estimer les coûts des attaques

Motif	***Valeur horaire (CAD 2016)***	***% de déplacements selon le motif***
Travail	18,56	49
Études	5,91	28
Autre - Conducteur	13,52	23
Autre – Passagers	9,50	4,6[8]

Pour estimer les coûts des attaques, nous nous sommes servis de l'information montrée antérieurement et nous avons procédé comme suit :

[7] Ces déplacements sont principalement réalisés par des parents qui déposent leurs enfants à l'école ou à la garderie [93].

[8] 20 % du 23 % des déplacements effectués pour un autre motif que travail ou études.

1. Pour chacune des attaques lancées contre des groupes de feux de circulation (combinaison type d'attaque et type de sélection des victimes), nous avons choisi le cas qui a produit l'impact négatif le plus important sur le temps perdu.
2. Les coûts des déplacements effectués pour les motifs travail ont été calculés en utilisant la formule suivante :

$$\text{Coût}_{\text{travail}} = \frac{\Delta\text{temps perdu moyen}}{3600} \times \text{Nbr. déplacements par heure} \times 1{,}2 \times 0{,}49 \times 18{,}52 \frac{\text{CAD}}{\text{h}}$$

3. Les coûts des déplacements effectués pour les motifs études ont été calculés en utilisant la formule suivante :

$$\text{Coût}_{\text{études}} = \frac{\Delta\text{temps perdu moyen}}{3600} \times \text{Nbr. déplacements par heure} \times 1{,}2 \times 0{,}28 \times 5{,}91 \frac{\text{CAD}}{\text{h}}$$

4. Les coûts des déplacements effectués pour autre motif ont été calculés en utilisant la formule suivante :

$$\text{Coût}_{\text{autre}} = \frac{\Delta\text{temps perdu moyen}}{3600} \times \text{Nbr. déplacements par heure} \times 0{,}23 \times (13{,}52 + 0{,}2 \times 9{,}50) \frac{\text{CAD}}{\text{h}}$$

5. Finalement, les coûts totaux estimés sont la somme des coûts résultants des trois calculs antérieurs.

Dans les formules présentées antérieurement, le terme *Δtemps perdu moyen* corresponde à la différence du temps perdu moyen obtenu pendant les attaques et le temps perdu moyen obtenu pour les conditions normales. Les valeurs résultantes des estimations des coûts pour les cas des attaques contre les groupes de feux de circulation ayant produit le plus d'impact sur le temps perdu son montrées au Tableau 6.6.

Étant donné que l'Attaque 1 contre groupes de feux de circulation choisis aléatoirement n'a pas produit d'impact négatif sur le temps perdu, nous n'avons pas estimé les coûts économiques de cette attaque.

Tableau 6.6 : Résultats des estimations des coûts des attaques qui ont produit le plus d'impact

	Cas 1	***Cas 2***	***Cas 3***
Temps perdu pour les conditions normales	153,20	153,20	153,20
Temps perdu durant l'attaque	157,16	199,60	215,36
Nombre de déplacements par heure	37 032	37 032	37 032
Coûts des déplacements effectués pour motif travail	444,55	5 208,92	6 978,16
Coûts des déplacements effectués pour motif études	80,89	947,81	1 269,73
Coûts des déplacements effectués pour un autre motif	140,91	1 651,08	2 211,88
Coûts totaux estimés par attaque (CAD/h)	**666**	**7 807**	**10 459**

Cas 1 : Attaque 1 ciblée contre les 20 feux de circulation les plus critiques
Cas 2 : Attaque 2 aléatoire contre 50 feux de circulation
Cas 3 : Attaque 2 ciblée contre les 50 feux de circulation les plus critiques

Les valeurs des coûts totaux montrées dans le Tableau 6.6 correspondent aux coûts résultant d'une d'attaque d'une heure de durée réalisée pendant la période des heures de pointe du matin.

Nous n'avons pas des données de référence avec lesquelles nous pourrions comparer les résultats obtenus des estimations des coûts économiques des attaques. Alors, nous ne pouvons pas confirmer la validité de ces résultats. Cependant, d'après les conditions de configuration de la simulation, nous pouvons inférer que les valeurs obtenues sont inférieures aux valeurs réelles causées par de vraies attaques. Une telle supposition est basée sur le fait que la demande de trafic simulée, bien qu'elle ait été générée à partir de données réelles, ne reproduit pas le vrai trafic dans le réseau. En fait, elle n'inclut ni les piétons, ni les cyclistes, ni les personnes se déplaçant en transport en commun, ni le camionnage, ni les déplacements des personnes non-résidentes dans la région de Montréal. C'est une partie importante du trafic urbain qui impacte le déroulement normal de la circulation dans les réseaux. En plus, la congestion incidente, résultante des chantiers et des accidents dans le réseau, n'a pas été simulée non plus.

D'autre part, l'estimation des coûts a été limitée aux coûts associés au temps perdu par les automobilistes, il manque les coûts de la consommation supplémentaire de carburant, des émissions supplémentaires des polluants et des gaz à effet de serre. Bien que ces deux composants manquants ne représentent qu'un pourcentage du coût total, ne pas les avoir incluses dans les estimations faites dans ce chapitre contribue à l'obtention de coûts inférieurs aux coûts réels.

Finalement, quant aux objectifs de recherche envisagés, cette section nous a permis d'atteindre le dernier des objectifs énoncés, c'est-à-dire, de mesurer les coûts économiques des attaques. Nous avons présenté une procédure qui est adoptée par des autorités publiques pour estimer les coûts de

la congestion routière. Nous nous sommes servis tant des valeurs obtenues de la simulation que des valeurs monétaires des certaines métriques, fournies par des autorités, pour aboutir à l'estimation du coût des attaques.

6.4 Conclusion

Dans ce chapitre nous avons présenté la démarche additionnelle que nous avons empruntée afin d'atteindre deux des objectifs spécifiques qui n'ont pas été atteints avec la démarche montrée au chapitre précédent. Ces objectifs étaient : reproduire expérimentalement l'état de la circulation dans un réseau routier de Montréal, dans les conditions normales et pendant des attaques informatiques contre les éléments du contrôle du trafic, et mesurer les coûts économiques des attaques. Pour ce faire, nous avons configuré dans SUMO le réseau routier, la demande du trafic et la programmation des feux de circulation du réseau routier du secteur municipal 101 de la Ville de Montréal. Ensuite, nous avons lancé deux types d'attaques contre les contrôleurs de feux de circulation sur le réseau : une attaque visant à désactiver les feux de circulation et l'autre visant à modifier les plans des feux, et nous avons utilisé deux stratégies de sélection des victimes : la sélection aléatoire et la sélection ciblée. Les victimes ciblées ont été identifiées en fonction du temps perdu moyen obtenu après des attaques individuelles de chaque feu de circulation dans le réseau. Puis, chaque attaque a été lancée deux fois contre des groupes de feux de circulation : une première fois en sélectionnant les feux aléatoirement et une deuxième fois en attaquant les feux qui avaient été identifiés comme étant les plus critiques (sélection ciblée). Cette expérimentation a fait ressortir que les attaques de modification des plans de feux ont des impacts négatifs plus grands sur le temps perdu que les attaques de désactivation des feux, et que l'impact augmente en fonction du nombre de feux attaqués. Aussi, les attaques contre les victimes ciblées produisent plus d'impact que les attaques où les victimes sont choisies aléatoirement, indépendamment du type d'attaque. Finalement, nous avons estimé les coûts des attaques pour les cas qui ont produit l'impact le plus important. L'estimation a été basée seulement sur les coûts associés au temps perdu, sans inclure les coûts associés à la consommation supplémentaire de carburant ni aux émissions supplémentaires de polluants et des gaz à effet de serre. Les valeurs obtenues correspondent aux coûts d'une heure d'attaque pendant la période des heures de pointe du matin.

Enfin, les démarches exécutées tant dans le chapitre 5 que dans ce chapitre, nous ont permis d'atteindre les objectifs énoncés au début de notre recherche. Le chapitre suivant portera sur la

discussion générale de la méthodologie adoptée, les résultats obtenus et leur lien avec les objectifs envisagés.

CHAPITRE 7 DISCUSSION GÉNÉRALE

Dans les chapitres 5 et 6 nous avons décrit la démarche exécutée afin d'atteindre les objectifs établis au début la recherche. Cette démarche visait à concevoir un scénario d'expérimentation permettant de mesurer les impacts d'attaques informatiques contre les systèmes qui contrôlent le trafic dans les réseaux routiers. Dans ce chapitre, nous présentons une analyse portant sur la méthodologie adoptée et sa pertinence avec les objectifs de recherche fixés.

7.1 Récapitulation des objectifs de la recherche

L'objectif principal de notre travail de recherche consiste à mesurer l'impact d'attaques informatiques sur le réseau de contrôle du trafic routier. Atteindre un tel objectif requiert premièrement de disposer d'un outil capable de reproduire tant les éléments qui contrôlent le trafic routier que le comportement du trafic dans les réseaux routiers. Cet outil nous permet, ultérieurement, de reproduire des attaques informatiques contre les éléments qui contrôlent le trafic routier et de mesurer les impacts de ces attaques. C'était dans cette optique que nous avons fixé les objectifs spécifiques suivants :

1. Développer un banc d'essai pour reproduire les systèmes contrôlant le trafic dans des réseaux routiers.
2. Reproduire expérimentalement des attaques informatiques contre les contrôleurs de feux de circulation d'un réseau routier.
3. Reproduire expérimentalement l'état de la circulation dans un réseau routier de Montréal en conditions normales et pendant une attaque informatique sur les feux de circulation.
4. Mesurer les coûts économiques des attaques, en fonction du retard global résultant de l'attaque sur le réseau.

Dans les sous-sections suivantes, nous présenterons une analyse critique de la méthodologie suivie et les choix que nous avons faits afin d'accomplir tous ces objectifs.

7.1.1 Développer un banc d'essai pour reproduire les systèmes contrôlant le trafic dans des réseaux routiers

À la section 5.5 nous avons décrit le banc d'essai que nous avons développé afin d'atteindre le premier des objectifs énoncés. Il est constitué par ScadaBR, une application logiciel open source qui émule les fonctions de la station centrale d'un système SCADA générique, SUMO, un logiciel open source de simulation microscopique qui reproduit le trafic dans les réseaux routiers, et des scripts python pour reproduire les PLC contrôlant les feux de circulation dans le réseau et le serveur qui communique les PLC avec l'interface de contrôle de SUMO. Ce banc d'essai est basé sur la co-simulation. Comme nous avons montré à la section 3.5.1 de ce mémoire, les bancs d'essai basés sur la co-simulation ont été amplement utilisés pour évaluer la sécurité informatique de divers systèmes de contrôle industriels. En raison de l'intégration du composant de contrôle et du composant physique (le processus contrôlé), les approches basées sur la co-simulation permettent d'évaluer comment le processus physique contrôlé est impacté par des attaques informatiques lancées contre le système de contrôle et ses composants. Une évaluation aussi globale ne serait pas possible en utilisant les approches basées seulement sur la simulation, car ces approches n'intègrent qu'un des composants du système étudié, soit le composant de contrôle ou le composant physique. En conséquence l'évaluation de la sécurité du système est limitée aux attaques qui peuvent être reproduites avec le composant simulé. Cela met en avant que la co-simulation offre plus de fidélité dans la composante cybernétique que les approches basées seulement sur la simulation, pour reproduire tant les attaques contre les systèmes de contrôle que les effets des attaques sur le processus physique. D'un autre côté, la co-simulation se révèle une option moins coûteuse en comparaison des autres approches, telles que les implémentations physiques. Dans certains cas, ces dernières requièrent d'importants investissements pour les construire (ou pour les reconstruire dans les cas de dommages résultants des tests), du personnel spécialisé pour les maintenir et les reconfigurer, voire d'autorisations réglementaires pour conduire certaines expériences [76].

7.1.2 Reproduire expérimentalement des attaques informatiques contre les contrôleurs de feux de circulation d'un réseau routier

Aux effets de notre travail, le banc d'essai devait avoir la capacité de reproduire une variété d'attaques informatiques contre le système et les composantes contrôlant le trafic, comme celles

montrées à la section 3.3.2 de ce mémoire. Cependant, l'usage de ScadaBR (pour simuler les fonctions du centre de gestion du trafic) au lieu d'un vrai logiciel de contrôle de trafic, qui utilise l'information récoltée sur le terrain pour calculer ou sélectionner les plans de feux, par exemple, limite les possibilités de reproduire certaines attaques visant à empêcher ou à altérer le fonctionnement du centre de gestion du trafic. Cela signifie que des attaques, telles que les attaques de déni de service contre le centre de gestion du trafic, ou de modification de l'information récoltée sur le terrain, ou des infections par vers ou virus informatiques, entre autres, n'ont pas pu être testées dans le scénario du banc d'essai développé. Nous avons utilisé le banc d'essai seulement pour reproduire d'attaques contre le réseau de communication, en exploitant les vulnérabilités du protocole Modbus utilisé pour communiquer entre ScadaBR et les PLC.

Pour ce faire, nous avons exploité les vulnérabilités de manque de chiffrement et d'authentification du protocole Modbus [45] [46] pour exécuter des attaques de l'homme au milieu, de rejeu[9] et d'injection de paquets[10] contre les PLC. Comme a été déjà démontré par Ghena *et al.* [13] et Cerrudo [14], les feux de circulation peuvent être manipulés en modifiant l'information transmise sur le réseau ou en insérant de faux (mais valides) messages dans le réseau. Alors, nous avons connecté une machine virtuelle Kali Linux (machine de l'attaquant) au même réseau des PLC et ScadaBR et nous avons utilisé des scripts python pour lancer les attaques. Pour les cas des attaques de l'homme au milieu, nous avons intercepté des réponses envoyées par le PLC à ScadaBR, les avons modifiées et les avons transmises à ScadaBR. Mais, en raison de la latence dans la communication générée par *scapy*, le protocole TCP a refusé certains des messages retransmis. Malgré cette circonstance, l'expérimentation a démontré que le banc d'essai permet l'exécution d'attaques de l'homme au milieu. De plus, les limitations relatives au timing de l'attaque illustrent bien la grande fidélité de la composante cybernétique de la co-simulation. Finalement, nous avons réussi à exécuter des attaques de rejeu et d'injection de paquets, et nous les avons utilisés pour

[9] Les attaques de l'homme au milieu et de rejeu ont été exécutées en utilisant la librairie *scapy* de python, qui permet la capture, modification et retransmission de messages dans un réseau.

[10] Les attaques d'injection de paquets ont été générées en utilisant la librairie *modbus-tk* de python, qui génère les messages des clients et serveurs Modbus.

altérer l'opération des feux de circulation dans deux configurations des réseaux routiers, comme nous l'avons montré à la section 5.6 de ce mémoire.

Bien que le scénario étudié dans le banc d'essai ne reproduise pas toutes les attaques informatiques qui peuvent être lancées contre le système et les éléments contrôlant le trafic, l'implémentation faite nous a permis de reproduire des attaques contre le réseau de communication qui ont mené à l'altération de l'opération des feux de circulation, ce qui nous permet d'atteindre les objectifs de recherche que nous nous étions fixés.

7.1.3 Reproduire l'état de la circulation dans un réseau routier de Montréal

Dans le chapitre précédent nous avons décrit la démarche additionnelle empruntée afin d'atteindre les objectifs qui n'ont pas été atteints avec la démarche présentée dans l'article. L'un de ces objectifs consistait à reproduire expérimentalement l'état de la circulation dans un réseau routier de Montréal, en conditions normales et pendant une attaque informatique sur les feux de circulation dans le réseau. C'est pour cela que nous avons reproduit dans SUMO une partie du réseau routier de la Ville de Montréal, spécifiquement le réseau routier du secteur municipal 101. La simulation a été configurée à partir des informations réelles, telles que la carte du réseau disponible sur OpenStreetMap, la demande du trafic pour les heures de pointe du matin et la programmation des feux de circulation dans le secteur. Nous avons aussi configuré la simulation avec certains paramètres qui ont ajouté le caractère stochastique à la simulation afin de reproduire la variabilité naturelle des comportements des conducteurs.

La demande du trafic a été simulée à partir de l'information contenue dans une matrice origine destination (matrice O-D) indiquant le nombre des déplacements ayant leur origine et/ou leur destination à l'intérieur du secteur. Cette information n'incluait que les déplacements faits en véhicules particuliers. Cela signifie que les piétons, les cyclistes, les personnes se déplaçant en transport en commun, le camionnage et les déplacements des personnes non-résidentes dans la région de Montréal n'ont pas été inclus. En plus, la congestion incidente, résultante des accidents, des travaux et des chantiers sur les rues, n'a pas été prise en compte non plus. Enfin, les modèles microscopiques du comportement des conducteurs n'ont pas été calibrés. En raison de ces limitations, le comportement du trafic simulé au cours de cette démarche pourrait ne pas refléter de vraies conditions de la circulation dans le secteur.

En dépit de ces conditions, nous avons réussi à reproduire un réseau routier de Montréal fidèle à la réalité (géométrie, plans de feux, etc.), et nous avons utilisé le réseau simulé pour reproduire des attaques contre les contrôleurs des feux de circulation.

7.1.4 Mesurer les coûts économiques des attaques

Pour atteindre ce dernier objectif, nous avons lancé des attaques d'injection de paquets sur le réseau de contrôle visant à altérer l'opération des feux de circulation de deux façons différentes : 1) désactiver les feux de circulation, et 2) modifier les plans des feux. Dans un premier temps, chaque attaque a été lancée individuellement contre tous les feux de circulation du secteur (un feu attaqué à la fois). Les résultats de ces attaques ont servi à classifier les feux de circulation et identifier ceux étant les plus critiques. Ensuite, chaque attaque a été lancée deux fois contre groupes de feux de circulation de taille de 5, 10, 20 et 50 feux. La première fois, les victimes ont été choisies aléatoirement. La deuxième fois, l'attaque a été lancée contre les 50 feux de circulation identifiés comme les plus critiques (sélection ciblée). À partir des résultats obtenus, nous avons identifié le cas (pour chaque combinaison de type d'attaque et type de sélection de victimes) qui a produit le plus d'impact négatif sur le temps perdu moyen et ces valeurs ont été utilisées pour estimer les coûts économiques des attaques.

En raison des limitations concernant la demande du trafic simulée qui ont été exprimées à la section précédente, les valeurs obtenues des estimations des coûts s'avèrent inférieures à celles qui seraient causées par de vraies attaques. Cependant, une telle déviation pourrait se corriger avec une calibration de la simulation mieux ajustée à la réalité. De plus, bien que les valeurs absolues calculées pour les attaques ne soient pas nécessairement valides, il a été possible de comparer de manière quantitatives diverses stratégies d'attaque ainsi que produire une évaluation de la criticité des feux de circulation du réseau pouvant être utilisée pour prioriser les défenses.

CHAPITRE 8 CONCLUSION ET RECOMMANDATIONS

Dans le chapitre précédent, nous avons fait une récapitulation des objectifs de notre recherche et nous avons présenté une analyse critique de la méthodologie suivie, en évaluant à quel point cette méthodologie nous a permis d'atteindre les objectifs proposés. Dans ce chapitre, consistant à conclure tout le travail réalisé, nous présenterons une synthèse de notre démarche, suivie par les limitations liées à la méthodologie adoptée et les contributions de notre travail, et enfin, des pistes qui pourraient être l'objet de recherches futures.

8.1 Synthèse des travaux

L'objectif principal de notre travail consistait à mesurer l'impact des attaques informatiques contre le réseau de contrôle du trafic routier. Pour atteindre cet objectif, nous avons tout d'abord développé un banc d'essai basé sur la co-simulation afin de reproduire un système contrôlant le trafic routier et le comportement du trafic dans les réseaux routiers. Ultérieurement, nous avons utilisé le banc d'essai pour reproduire des attaques informatiques contre le système de contrôle du trafic et mesurer l'impact des attaques.

Le banc d'essai se compose de :

- ScadaBR, une application à code ouvert qui émule la station centrale d'un système SCADA et qui a agi comme le centre de gestion du trafic ;
- Scripts python qui ont reproduit les fonctions des PLC contrôlant les feux de circulation ;
- SUMO, un logiciel à code ouvert de simulation microscopique du trafic qui a permis la modélisation des réseaux routiers et du trafic ; et
- Un serveur TCP développé en python qui a établi la communication entre les PLC et l'interface de contrôle de SUMO.

Pour contrôler les feux de circulation, nous avons reproduit une logique de contrôle tirée de la littérature, et nous avons utilisé le protocole de communication industriel Modbus/TCP pour implémenter la communication entre ScadaBR et les PLC.

Dans un premier temps, nous avons configuré un réseau routier générique composé de trois carrefours à feux, chacun d'eux étant contrôlé par un PLC, et nous avons lancé une attaque d'injection de paquets dans le réseau de contrôle qui a désactivé le feu de circulation du premier carrefour à feux. Toute cette expérimentation a été exécutée depuis un ordinateur de bureau, en utilisant des machines virtuelles pour exécuter ScadaBR, chacun des PLC et la machine de l'attaquant (une machine Kali Linux). L'impact de l'attaque a été mesuré en fonction de la longueur des files d'attente sur les tronçons du réseau. Cette expérimentation a fait ressortir que l'attaque a produit une augmentation non seulement de la file d'attente au carrefour attaqué, mais aussi aux carrefours adjacents.

Deuxièmement, nous avons reproduit un corridor routier dont les six feux de circulation sont coordonnés afin de favoriser la circulation des flux se déplaçant de l'ouest vers l'est. Nous avons utilisé un PLC pour contrôler le carrefour à feux à l'entrée ouest du corridor, qui était le carrefour de référence du système, et un autre PLC pour contrôler l'avant-dernier carrefour à feux du corridor, qui a été le carrefour attaqué. En raison des limitations de la puissance de l'ordinateur utilisé, les autres carrefours à feux ont été contrôlés depuis la simulation. Ensuite, nous avons lancé une attaque d'injection de paquets dans le réseau de contrôle qui a réduit à la moitié la durée du feu vert des deux phases du plan du feu attaqué. L'impact de l'attaque a été mesuré en fonction du temps de parcours des voitures traversant le corridor de l'ouest vers l'est et de la longueur des files d'attente sur les tronçons du corridor. Similairement à la première expérimentation, l'attaque a impacté le temps de parcours et la longueur de la file d'attente non seulement sur l'approche convergeant vers le carrefour attaqué, mais aussi sur tous les tronçons se trouvant à l'ouest du carrefour attaqué, ce qui s'est traduit par une augmentation du temps de parcours. Le fait que notre approche permet d'observer ces effets sur les carrefours n'ayant pas été directement attaqués démontre l'importance de la co-simulation dans le cadre de systèmes cyber-physiques.

Troisièmement, nous avons modélisé une partie du réseau routier de la Ville de Montréal à partir de données réelles. Nous avons exécuté des attaques de désactivation des feux et de modification des plans des feux tant contre chacun des carrefours à feux du réseau individuellement que contre groupes de carrefours à feux. Les attaques individuelles nous ont servi pour classer les carrefours à feux selon leur criticité, laquelle a été attribuée en fonction du temps perdu moyen résultant de la simulation de l'attaque contre chaque carrefour à feux. Pour les attaques par groupes, nous avons utilisé deux stratégies de sélection des victimes : la sélection aléatoire et la sélection ciblée, où les

victimes ont été les 50 carrefours à feux identifiés comme les plus critiques. Cette expérimentation a mis en évidence que les attaques de désactivation des feux produisent une diminution du temps perdu (impact positif) qui augmente en fonction du nombre de carrefours à feux attaqués, que les attaques de modification des plans de feux produisent une augmentation du temps perdu (impact négatif) qui augmente en fonction du nombre de carrefours à feux attaqués, et que les attaques contre des groupes de carrefours à feux ciblés produisent plus d'impact négatif sur le temps perdu que les attaques contre des cibles choisies de façon aléatoire, indépendamment du type d'attaque. Ceci démontre que notre approche permet d'évaluer la performance de différentes stratégies dans un environnement représentatif du monde réel.

Finalement, nous avons estimé les coûts économiques résultants des attaques contre le réseau de la Ville de Montréal modélisé selon le temps perdu par les usagers et la valeur du temps utilisée dans les études de la région de Montréal. Les coûts ont été estimés pour les cas des attaques lancées contre groupes de carrefours à feux qui ont produit le plus d'impact négatif sur le temps perdu.

8.2 Limitations

Tout d'abord, le banc d'essai a démontré être performant pour reproduire des attaques informatiques contre le réseau de communication en exploitant les vulnérabilités du protocole Modbus. Cependant, le fait de ne pas avoir utilisé un vrai logiciel de contrôle du trafic et des vrais PLC a limité la capacité du banc d'essai de reproduire des attaques informatiques. Par exemple, les attaques de déni de service contre le centre de gestion du trafic, et les infections par vers ou virus informatiques contre tant le centre de gestion du trafic que les PLC n'ont pas pu être testées.

L'attaque de modification des plans de feux lancée contre les feux de circulation du secteur municipal 101 de la Ville de Montréal a produit des impacts subtils sur le temps perdu, ce qui signifie qu'il faudra essayer d'autres façons de modifier les plans de feux (différentes à dupliquer la durée du cycle des feux) afin d'évaluer l'impact sur le temps perdu. Aussi, nous avons déterminé les feux de circulation étant les plus critiques en raison du temps perdu moyen résultant des attaques individuelles sur chaque feu de circulation. Il serait nécessaire d'essayer d'autres critères pour déterminer les feux de circulation les plus critiques et évaluer l'impact de la sélection sur le temps perdu.

La calibration de la simulation du trafic dans le secteur de la Ville de Montréal attaqué a présenté certaines limitations qui pourraient produire des résultats qui ne reflètent pas la réalité. D'abord, la demande du trafic qui nous a été fournie, bien qu'elle soit réelle, n'inclut pas les piétons, les cyclistes, les personnes se déplaçant en transport en commun, le camionnage, la livraison locale et les déplacements des personnes non résidentes dans la région de Montréal. En plus, la congestion incidente, résultante des accidents, des travaux et des chantiers sur les rues n'a pas été prise en compte non plus. Deuxièmement, la calibration du comportement des conducteurs n'a pas été faite. Troisièmement, l'activation de la possibilité pour les usagers de changer d'itinéraire (« rerouting »), afin de régler les problèmes des déplacements qui n'avaient pas d'itinéraires valides, a permis que la simulation recalcule et adapte périodiquement les routes attribuées aux véhicules en fonction de l'état courant de la circulation dans le réseau. Dans cette condition, les conducteurs ont pu éviter les embouteillages et, en conséquence, auraient perdu moins de temps dans leur parcours.

Les estimations des coûts économiques des attaques contre le réseau de la Ville de Montréal modélisé ont présenté aussi des limitations qui impactent les résultats obtenus. D'un côté, elles n'ont pas inclus les coûts associés à la consommation supplémentaire du carburant, les émissions de polluants et les émissions des gaz à effet de serre, car la flotte de véhicules n'a pas été calibrée selon le parc automobile du secteur modélisé (différents types de moteurs, âge de la flotte, véhicules électriques, etc.). D'un autre côté, les estimations ont considéré seulement le temps perdu des véhicules particuliers se déplaçant dans le secteur pendant la période étudiée.

Les limitations, quant aux types d'attaques informatiques qui peuvent être reproduits et la validité des résultats obtenus dans le banc d'essai actuel, peuvent être réglées en remplaçant ScadaBR par un vrai logiciel de contrôle de trafic et en ajustant la calibration de la simulation. Cela augmenterait la fidélité du banc d'essai et aussi sa capacité à reproduire d'autres attaques informatiques en plus de celles qui ont été exécutées dans ce travail.

8.3 Contributions

La principale contribution de notre travail est le banc d'essai basé sur la co-simulation qui permet de reproduire des attaques informatiques contre le réseau de contrôle du trafic routier et de mesurer les impacts des attaques. C'est un outil à faible coût, qui combine des applications à code ouvert et des scripts développés en python qui le rendent disponible et réutilisable sans exiger des paiements

de licences. En plus, tous ses composants peuvent fonctionner sur le système d'exploitation tant Windows que Linux, ce qui ne limite pas son usage à un système d'exploitation particulier.

De plus, l'intégration du composant de contrôle et du processus physique dans le banc d'essai offre la possibilité de lancer des attaques informatiques contre les éléments qui contrôlent le trafic routier, et de mesurer comment les attaques impactent la circulation. C'est sans doute l'un des avantages de la co-simulation par rapport à d'autres approches, comme les approches basées sur la simulation d'un seul composant du système.

Ces contributions ont fait l'objet d'une publication dans une conférence revue par les pairs.

De plus, bien que les valeurs absolues résultantes de la simulation soient potentiellement peu représentatives de la réalité, nous avons aussi présenté une évaluation de l'impact d'attaques informatiques dans un cas réel. Cette évaluation a permis de comparer de différentes stratégies d'attaques pour différentes capacités de l'attaquant, ce qui pourrait servir aux autorités à établir ou renforcer les mesures de sécurité visant à se protéger contre les attaques pouvant produire le plus d'impact.

8.4 Travaux futurs

Bien que l'objectif de mesurer l'impact des attaques informatiques contre le réseau de contrôle du trafic routier ait été atteint, le banc d'essai développé pourrait aussi servir de point de départ pour des recherches futures dans le domaine de la sécurité des systèmes de contrôle de trafic routier, ou d'autres systèmes.

Tout d'abord, des ajustements à la calibration de la simulation seront nécessaires afin de reproduire les conditions du trafic dans le réseau les plus proches à la réalité. Il faudra inclure aussi dans la calibration l'information du parc automobile du secteur et des modèles de la consommation d'essence, des émissions de polluants et des émissions des gaz à effet de serre. Une telle calibration permettrait d'avoir des estimations des coûts économiques des attaques plus complètes.

Augmenter la capacité du banc d'essai de reproduire des attaques informatiques sera aussi nécessaire afin de pouvoir lancer des attaques contre le centre de gestion du trafic et mesurer l'impact de ces attaques. Une des façons de le faire serait en intégrant un logiciel de contrôle de trafic au lieu d'utiliser ScadaBR.

Nous suggérons aussi d'essayer d'autres attaques de modification des plans de feux, plus sophistiquées, que celles qui ont été exécutées dans ce travail, ou d'utiliser d'autres critères, par exemple le rapport d'accidents de chaque carrefour à feu, pour déterminer les feux de circulation les plus critiques. Après, évaluer l'impact des attaques avec ces nouvelles conditions.

Finalement, le banc d'essai pourrait être utilisé pour étudier des mécanismes de défense visant à détecter ou empêcher les attaques qui attentent à l'intégrité ou à l'authentification de l'information échangée par le centre de gestion du trafic et les PLC.

RÉFÉRENCES

[1] Affaires environnementales Transports Canada, «Le Coût de la congestion urbaine au Canada,» Transports Canada, Canada, 2006.

[2] Ministère des Transports du Québec et Les Conseillers ADEC inc., «Évaluation des coûts de la congestion routière dans la région de Montréal pour les conditions de référence de 2008,» Montreal. Canada, 2014.

[3] R. H. White, J. D. Spengler, K. M. Dilwali, B. E. Barry et J. M. Samet, «Report of Workshop on Traffic, Health, and Infrastructure Planning,» *Archives of Environmental & Occupational Health*, vol. 60, n° %12, pp. 70-76, 2005.

[4] J. I. Levy, J. J. Buonocore et K. Von Stackelberg, «Evaluation of the public health impacts of traffic congestion: a health risk assessment,» *Environmental health*, vol. 9, n° %11, p. 65, 2010.

[5] INRIX, «INRIX Global Traffic Scorecard,» INRIX, 2017.

[6] TomTom International BV, «TomTom Traffic Index 2017: Mexico City Retains Crown of 'Most Traffic Congested City' in World,» 21 2 2017. [En ligne]. Available: http://corporate.tomtom.com/releasedetail.cfm?releaseid=1012517. [Accès le 5 10 2017].

[7] Ontario Traffic Council, «Advance Traffic Management Systems,» chez *Ontrario Traffic Manual*, Toronto, Canada, 2007.

[8] The Roadmap to Secure Control Systems in the Transportation Sector Working Group, «Roadmap to Secure Control Systems in the Transportation Sector,» Exponsored by the U.S. Department of Homeland Security's National Cybersecurity Division and the Control Systems Security Program, 2012.

[9] Boston Transportation Department & Howard/Stein-Hudson Associates , Inc., «The benefits of retiming/rephasing traffic signals in the Back Bay,» Boston Transportation Department, Boston, USA, 2010.

[10] City of Bloomington, «Signal Timing Optimization and Coordination,» Alliant Engineering Inc., Bloomington, USA, 2012.

[11] F. Siddiqui, «The Washington Post,» 8 8 2015. [En ligne]. Available: https://www.washingtonpost.com/local/could-a-hacker-gain-control-of-dcs-traffic-system/2015/08/08/7cb7cf94-201a-11e5-bf41-c23f5d3face1_story.html?utm_term=.73f4833262b7. [Accès le 8 12 2017].

[12] Vandita, «ANONHQ.COM,» 2 8 2015. [En ligne]. Available: http://anonhq.com/when-two-engineers-hacked-las-signal-system-wreaked-havoc-on-streets/. [Accès le 8 12 2017].

[13] B. Ghena, W. Beyer, A. Hillaker, J. Pevarnek et J. A. Halderman, «Green Lights Forever: Analyzing the Security of Traffic Infrastructure,» chez *8th USENIX Workshop on Offensive Technologies*, San Diego, USA, 2014.

[14] C. Cerrudo, «Hackers Can Mess With Traffic Lights to Jam Roads and Reroute Cars,» 30 04 2014. [En ligne]. Available: https://www.wired.com/2014/04/traffic-lights-hacking/. [Accès le 15 04 2017].

[15] National Transportation Operations Coalition, «Traffic Signals 101,» [En ligne]. Available: http://www.bceo.org/departments/engineering/Traffic-Signals101.pdf.

[16] Minnesota Department of Transportation, «Traffic Signals 101,» Minnesota Department of Transportation, Minneapolis, USA, 2015.

[17] The Vehicle Detector Clearinghouse, «Summary of vehicle detection and surveillance technologies used in intelligent transportation systems,» Federal Highway Administration’s Intelligent Transportation Systems Joint Program Office, 2000.

[18] M. Tubaishat, Y. Shang et H. Shi, «Adaptive Traffic Light Control with Wireless Sensor Networks,» chez *Proceedings of IEEE Consumer Communications and Networking Conference*, Las Vegas, USA, 2007.

[19] S. Faye, «Contrôle du trafic routier urbain par un réseau fixe de capteurs sans fil,» Télécom ParisTech, Paris, France, 2012.

[20] K. M. Yousef, J. N. Al-Karaki1 et A. M. Shatnawi, «Intelligent Traffic Light Flow Control System Using Wireless Sensors Networks,» *Journal of Information Science and Engineering*, vol. 26, pp. 753-768, 2010.

[21] S. Coleri, S. Y. Cheung et P. Varaiya, «Sensor Networks for Monitoring Traffic,» chez *42nd Annual Allerton Conference on Communication, Control, and Computing*, Monticello, Illinois, 2004.

[22] Federal Highway Administration, «Signalized Intersections Informational Guide, Second Edition,» U.S. Department of Transportation, Washington, D.C., 2013.

[23] Federal Highway Administration, «Traffic control systems handbook,» Federal Highway Administration, Washington, USA, 2005.

[24] Federal Highway Administration & Dunn Engineering Associates, P.C., «Traffic Control Systems Handbook,» Federal Highway Administration, Washington, DC, USA, 2005.

[25] U.S. Department of Transportation, «Traffic signal timing manual,» Federal Highway Administration, McLean, USA, 2008.

[26] P. B. Hunt, D. I. Roberston, R. D. Bretherton et R. I. Winton, «SCOOT - A TRAFFIC RESPONSIVE METHOD OF COORDINATING SIGNALS,» Transport and Road Research Laboratory, United Kingdom, 1981.

[27] A. G. Sims et K. W. Dobinson, «The Sydney Coordinated Adaptive Traffic (SCAT) System. Philosophy and Benefits,» *IEEE Transactions on Vehicular Technology,* vol. 29, n° %12, pp. 130-137, 1980.

[28] N. H. Gartner, «OPAC: Strategy for Demand-Responsive Decentralized Traffic Signal Control,» chez *IFAC/IFIP/IFORS Symposium*, Paris, 1989.

[29] J. J. Henry, J. L. Farges et J. Tuffal, «The PRODYN Realtime Traffic Algorithm,» *IFAC Control in Transportation Systems,* pp. 305-310, 1983.

[30] R. L. Gordon, R. A. Reiss, W. M. Dunn et D. R. Morehead, «Communications Handbook for Traffic Control Systems,» U.S. Department of Transportation, Federal Highway Administration, Washington, DC, 1993.

[31] Federal Highway Administration, «Traffic Signal Control Systems,» chez *Advanced Transportation Management Technologies*, U. S. Department of Transportation, 1997, pp. 3-1, 3-28.

[32] J. Caswell, «Survey of Industrial Control Systems Security,» 12 08 2011. [En ligne]. Available: http://www.cse.wustl.edu/~jain/cse571-11/ftp/ics/index.html. [Accès le 12 02 2018].

[33] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams et A. Hahn, «Guide to Industrial Control Systems (ICS) Security,» National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Maryland, USA, 2015.

[34] E. Hayden, M. Assante et T. Conway, «An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity,» SANS Institute, 2014.

[35] R. C. Dorf et R. H. Bishop, «Introduction to Control Systems,» chez *Modern Control Systems, 12th edition*, Prentice Hall, 2011, pp. 2-34.

[36] A. Cardenas, S. Amin et S. Sastry, «Research challenges for the security of control systems,» chez *3rd USENIX Workshop on Hot Topics in Security, HotSec'08,* San Jose, CA, 2008.

[37] Trend Micro Inc., «Industrial Control Systems,» [En ligne]. Available: https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system. [Accès le 05 02 2018].

[38] J. Weiss, «Assuring Industrial Control System (ICS) Cyber Security,» [En ligne]. Available: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/080825_cyber.pdf. [Accès le 05 02 2018].

[39] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A.-R. Sadeghi, M. Maniatakos et R. Karri, «The Cybersecurity Landscape in Industrial Control Systems,» *Proceedings of the IEEE,* vol. 104, n° %15, pp. 1039-1057, 2016.

[40] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang et S. Sastry, «Attacks Against Process Control Systems: Risk Assessment, Detection, and Response,» chez *AsiaCCS,* Hong Kong, 2011.

[41] Symantec, «Internet Security Threat Report,» Symantec, 2016.

[42] D. Pidikiti, R. Kalluri, R. Kumar et B. Bindhumadhava, «SCADA communication protocols: vulnerabilities, attacks and possible mitigations,» *CSI Transactions on ICT (CSIT),* vol. 1, n° %12, pp. 135-141, 2013.

[43] European Network and Information Security Agency (ENISA), «Protecting Industrial Control Systems. Recommendations for Europe and Member States,» 2011.

[44] M. Herrero Collantes et A. López Padilla, «Protocols and network security in ICS infrastructures,» Spanish National Cybersecurity Institue , 2015.

[45] Q. Wanying, W. Weimin, Z. Surong et Z. Yan, «The Study of Security Issues for the Industrial Control Systems Communication Protocols,» chez *Joint International Mechanical Electronic and Information Technology Conference (JIMET)*, Chongqing China, 2015.

[46] G. Jakaboczki et E. Adamko, «Vulnerabilities of Modbus RTU Protocol - A case study,» *Management and Technological Engineering*, n° %11, pp. 203-206, 2015.

[47] National Cyber Security Division's Control Systems Security Program, «Common Cyber Security Vulnerabilities Observed in DHS Industrial Control Systems Assessments,» U.S. Department of Homeland Security, 2009.

[48] S. Nazir, S. Patel et D. Patel, «Assessing and augmenting SCADA cyber secur ity: A survey of techniques,» *Computer & Security* , vol. 70, pp. 436-454, 2017.

[49] D. Dzung, M. Naedele, T. Von Hoff et M. Crevatin, «Security for Industrial Communication Systems,» *PROCEEDINGS OF THE IEEE*, vol. 93, n° %16, pp. 1152-1177, 2005.

[50] National Cyber Security Division, «Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability,» U.S. Department of Homeland Security, 2009.

[51] A. Cui et S. J. Stolfo, «A Quantitative Analysis of the Insecurity of Embedded Network Devices: Results of a Wide-Area Scan,» chez *Annual Computer Security Applications Conference*, Austin, Texas, 2010.

[52] 0patch Blog, «Security Patching is Hard - Survey Results 2017,» 30 03 2018. [En ligne]. Available: https://0patch.blogspot.ca/2018/03/security-patching-is-hard-survey.html. [Accès le 08 04 2018].

[53] M. Masera, I. N. Fovino et R. Leszczyna, «Security assessment of a turbo-gas power plant,» *Critical Infrastructure Protection II,* vol. 290, pp. 31-40, 2008.

[54] K. Zetter, «SCADA System's Hard-Coded Password Circulated Online for Years,» 2010 07 19. [En ligne]. Available: https://www.wired.com/2010/07/siemens-scada/. [Accès le 15 02 2018].

[55] E. Byres, «Patching for SCADA and ICS Security: The Good, the Bad and the Ugly,» 26 03 2013. [En ligne]. Available: https://www.tofinosecurity.com/blog/patching-scada-and-ics-security-good-bad-and-ugly. [Accès le 27 02 2018].

[56] K. Zetter, «Attack Code for SCADA Vulnerabilities Released Online,» 22 03 2011. [En ligne]. Available: https://www.wired.com/2011/03/scada-vulnerabilities/. [Accès le 15 02 2018].

[57] E. Mills, «Researchers warn of SCADA equipment discoverable via Google,» 02 08 2011. [En ligne]. Available: https://www.cnet.com/news/researchers-warn-of-scada-equipment-discoverable-via-google/. [Accès le 15 02 2018].

[58] M. E. Luallen, «Critical Control System Vulnerabilities Demonstrated - And What to Do About Them,» SANS Institute, Chicago, USA, 2011.

[59] L. Poinsot, «Chap. I : Introduction à la sécurité informatique,» [En ligne]. Available: http://www.univ-tebessa.dz/fichiers/master/master_951.pdf. [Accès le 05 04 2017].

[60] Wikipedia, «Computer security,» 01 03 2018. [En ligne]. Available: https://en.wikipedia.org/wiki/Computer_security. [Accès le 02 03 2018].

[61] S. Ghernaouti, «Principes de sécurité,» chez *Cybersécurité. Sécurité informatique et réseaux - 4e édition*, Paris, DUNOD, 2016, pp. 1-17.

[62] C. E. Landwehr, «Computer security,» *International Journal of Information Security,* vol. 1, n° %11, p. 3–13, 2001.

[63] W. Stallings, «Introduction,» chez *Network Security Essencials: Applications and Standards. Fourth Edition*, Upper Saddle River, Prentice Hall, 2011, pp. 1-26.

[64] S. Gill, «Type d'attaques,» 27 05 2013. [En ligne]. Available: https://fr.scribd.com/document/143959383/Type-Attaques. [Accès le 05 04 2017].

[65] Wikipedia, «Ingénierie sociale (sécurité de l'information),» [En ligne]. Available: https://fr.wikipedia.org/wiki/Ing%C3%A9nierie_sociale_(s%C3%A9curit%C3%A9_de_l%27information). [Accès le 26 03 2018].

[66] S. Hansman et R. Hunt, «A taxonomy of network and computer attacks,» *Computers & Security*, vol. 24, n° %11, pp. 31-43, 2005.

[67] E. Cole, «The Changing Threat,» chez *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization*, Waltham, Syngress, 2013, pp. 3- 26.

[68] Wikipedia, «Advanced persistent threat,» Wikipedia, 4 12 2017. [En ligne]. Available: https://en.wikipedia.org/wiki/Advanced_persistent_threat. [Accès le 05 03 2018].

[69] J. Slay et M. Miller, «Lessons Learned from the Maroochy Water Breach,» *International Conference on Critical Infrastructure Protection*, vol. 253, pp. 73-82, 2008.

[70] N. Falliere, L. O. Murchu et E. Chien, «W32.Stuxnet Dossier (version 1.4),» Symantec Security Response, 2011.

[71] P. Mueller et B. Yadegari, «The Stuxnet Worm,» [En ligne]. Available: https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf. [Accès le 06 03 2018].

[72] R. M. Lee, M. J. Assante et T. Conway, «German Steel Mill Cyber Attack,» SANS Industrial Control Systems, 2014.

[73] SANS Industrial Control Systems (SANS ICS), «TLP: White. Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case,» Electricity Information Sharing and Analysis Center (E-ISAC), Washington, D.C., 2016..

[74] K. Zetter, «Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid,» 03 03 2016. [En ligne]. Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. [Accès le 22 03 2016].

[75] Y.-L. Huang, A. A. Cárdenas, S. Amin, Z.-S. Lin, H.-Y. Tsai et S. Sastry, «Understanding the physical and economic consequences of attacks on control systems,» *International Journal of Critical Infrastructure Protection,* vol. 2, n° %13, pp. 73-83, 2009.

[76] M. Krotofil et J. Larsen, «Rocking the pocket book: Hacking chemical plants for competition and extortion,» chez *DEF CON 23*, Las Vegas, USA, 2015.

[77] G. Bernieri, E. E. Miciolino, F. Pascucci et R. Setola, «Monitoring system reaction in cyber-physical testbed under cyber-attacks,» *Computers & Electrical Engineering,* 2017.

[78] C. Heracleous, E. Etchevés M., R. Setola, F. Pascucci, D. Eliades, G. Ellinas et M. Panayiotou, «Critical Infrastructure Online Fault Detection: Application in Water Supply Systems,» chez *9th International Conference, Critical Information Infrastructures Security (CITRIS 2014)*, Limassol, Cyprus, 2014.

[79] A. Lemay, J. Fernandez et S. Knight, «An isolated virtual cluster for SCADA network security research,» chez *1st International Symposium for ICS & SCADA Cyber Security Research*, Leicester, UK, 2013.

[80] J. Calvet, C. R. Davis, J. M. Fernandez, W. Guizani, M. Kaczmarek, J.-Y. Marion et P.-L. St-Onge, «Isolated Virtualised Clusters: Testbeds for High-Risk Security Experimentation and Training,» chez *3rd Workshop on Cyber Security Experimentation and Test (CSET'10)*, Washington, USA, 2010.

[81] J. M. Ernst et A. J. Michaels, «A Framework for Evaluating the Severity of a Traffic Cabinet Cyber Vulnerability,» Washington DC, USA, 2017.

[82] D. Krajzewicz, G. Hertkorn, C. Rössel et P. Wagner, «SUMO (Simulation of Urban MObility)-an open-source traffic simulation,» chez *4th Middle Eastern Symposium on Simulation and Modelling (MESM2002)*, Dubai, 2002.

[83] B. C. Ezell, R. M. Robinson, P. Foytik, C. Jordan et D. Flanagan, «Cyber risk to transportation, industrial control systems, and traffic signal controllers,» *Environment Systems and Decisions*, vol. 33, n° %14, p. 508–516, 2013.

[84] J. M. Ernst et A. J. Michaels, «A Framework for Evaluating the Severity of a Traffic Cabinet Cyber Vulnerability,» chez *2016 Transport Reseach Board Annual Meeting*, Washington, D.C., 2016.

[85] M. Krotofil et A. D, «Hack Like a Movie Star,» 2015. [En ligne]. Available: http://2015.zeronights.org/assets/files/12-Krotofil.pdf. [Accès le 19 05 2017].

[86] «ScadaBR,» [En ligne]. Available: http://www.scadabr.com.br/. [Accès le 15 11 2016].

[87] Python, «Package Index > modbus_tk > 0.5.7,» Phyton Software Foundation (US), [En ligne]. Available: https://pypi.python.org/pypi/modbus_tk. [Accès le 19 05 2017].

[88] Réseau de transport métropolitain, «Enquête OD 2013,» [En ligne]. Available: https://rtm.quebec/fr/a-propos/portrait-mobilite/enquete-od-2013. [Accès le 25 03 2018].

[89] Dkrajzew, «SUMO User Documentation,» 12 12 2008. [En ligne]. Available: http://sumo.dlr.de/wiki/OD2TRIPS. [Accès le 15 01 2017].

[90] J. Erdmann, «SUMO's Lane-Changing Model,» chez *Modeling Mobility with Open Data. Lecture Notes in Mobility*, Berlin, Springer, 2015, pp. 105-123.

[91] L. Gauthier, «Méthode de calibration des logiciels de microsimulation routière à l'aide de l'optimisation sans dérivées,» Université de Montréal, Montréal, 2015.

[92] Ministère des Transports, de la Mobilité durable et de l'Électrification des transports, «Guide de l'analyse avantages- coûts des projets publics en transport routier. Paramètres (Valeurs de 2015),» Gouvernement du Québec, Québec, 2016.

[93] Réseau de transport métropolitain, «La mobilité des personnes dans la région de Montréal. FAITS SAILLANTS,» [En ligne]. Available: https://rtm.quebec/Media/Default/pdf/section8/enquete-od-2013-faits-saillants.pdf. [Accès le 25 03 2018].

[94] A. Arfaoui, «Estimation des matrices origine-destination à partir des comptages : Étude de quelques modèles,» Institute National de Recherche sur les Transports et leur Sécurité, France, 1999.

[95] Wikipedia, «OpenStreetMap,» 14 03 2018. [En ligne]. Available: https://en.wikipedia.org/wiki/OpenStreetMap.

[96] Wikipédia, «Produit informatique standard,» [En ligne]. Available: https://fr.wikipedia.org/wiki/Produit_informatique_standard. [Accès le 06 02 2018].